

No. 2023-1129

---

# United States Court of Appeals for the Federal Circuit

---

CUPP COMPUTING AS,  
*Appellant,*

v.

TREND MICRO INC.,  
*Appellee.*

---

Appeal from the United States Patent and Trademark Office,  
Patent Trial and Appeal Board, in No. IPR2021-00813

---

**OPENING BRIEF FOR  
APPELLANT CUPP COMPUTING AS**

---

Paul J. Andre  
James Hannah  
KRAMER LEVIN NAFTALIS &  
FRANKEL LLP  
333 Twin Dolphin Drive  
Suite 700  
Redwood Shores, CA 94065  
Telephone: (650) 752-1700

Jeffrey Price  
KRAMER LEVIN NAFTALIS &  
FRANKEL LLP  
1177 Avenue of the Americas  
New York, NY 10036  
Telephone: (212) 715-7502

***ATTORNEYS FOR CUPP COMPUTING AS***

---

**PATENT CLAIMS AT ISSUE**

**U.S. Patent No. 10,621,344**

8. The security system of claim 1, wherein the security code, the security policy, and the security data are configured to mirror security policies of a gateway on the trusted enterprise network.

17. The non-transitory computer readable storage device of claim 10, wherein the security code, the security policy, and the security data are configured to mirror security policies of a gateway on the trusted enterprise network.

19. A security system, comprising:

security system memory; and

a security system processor configured to:

store in the security system memory at least a portion of security code, at least a portion of a security policy, and at least a portion of security data,

the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to be processed by the security system processor to implement security services for a mobile device coupled to the security system, the mobile device having at least one mobile device processor different than the security system processor of the security system,

the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being managed by one or more information technology (IT) administrators using an IT administrator system on a trusted enterprise network, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network, the mobile device being a first computer system, the security system being a second computer system, and the IT administrator system being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems;

store in the security system memory at least a portion of remote management code configured to process an update command, the update command being an instruction to update at least one of the security code, the security policy, or the security data based on one or more revised policies implemented by the one or more IT administrators on the trusted enterprise network;

receive a particular update command to update a particular one of the security code, the security policy, or the security data, the particular update command having originated from the IT administrator system and having been forwarded to the security system; and

execute the update command using the remote management code to update the particular one of the security code, the security policy, or the security data.

20. A non-transitory computer readable storage device of a security system storing:

program instructions;

at least a portion of security code, at least a portion of a security policy, and at least a portion of security data,

the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to be processed by the security system processor to implement security services for a mobile device coupled to the security system, the mobile device having at least one mobile device processor different than the security system processor of the security system,

the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being managed by one or more information technology (IT) administrators using an IT administrator system on a trusted enterprise network, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network, the mobile device being a first computer system, the security system being a second computer system, and the IT administrator system being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems; and

at least a portion of remote management code configured to process an update command, the update command being an instruction to update at least one of the security code, the security policy, or the security data based on one or more revised policies implemented by the one or more IT administrators on the trusted enterprise network;

the program instructions when executed by the security system processor causing the security system to receive a particular update command to update a particular one of the security code, the security policy, or the security data, the particular update command having originated from the IT administrator system, the particular update command having been forwarded to the security system; and

the remote management code when executed by the security system processor causing the system to process the update command to update the particular one of the security code, the security policy, or the security data.

**CERTIFICATE OF INTEREST**

Counsel for CUPP Computing AS certifies the following:

1. The full name of every entity represented by us is:

CUPP Computing AS

2. For each entity, the name of every real party in interest, if that entity is not the real party in interest. Do not list the real party if it is the same as the entity:

Not applicable.

3. All parent corporations and any other publicly held companies that own 10 percent or more of the stock of the entity represented by us are listed below:

Not applicable.

4. The names of all law firms, and the partners or associates that have not entered an appearance in the appeal, and (a) appeared for the entity in the lower tribunal; or (b) are expected to appear for the entity in this court:

Jenna Fuller of Kramer Levin Naftalis & Frankel LLP

5. Other than the originating case number(s), are there related or prior cases that meet the criteria under Fed. Cir. R. 47.5(a)?

- whether any other appeal in or from the same civil action or proceeding in the originating tribunal was previously before this or any other appellate court:

*CUPP Computing AS v. Trend Micro Inc.*, No. 20-2059 (Fed. Cir. Oct. 6, 2022) (Dyk, Taranto, and Stark, Circuit Judges). The decision was not published in the Federal Reporter.

- the title and number of any case known to counsel to be pending in this or any other tribunal that will directly affect or be directly affected by this court's decision in the pending appeal:

*CUPP Cybersecurity, LLC v. Trend Micro, Inc. et al.*, No. 3:18-cv-01251 (N.D. Tex.) (consolidated with 3:20-cv-03206 (N.D. Tex.)).

6. All information required by Fed. R. App. P. 26.1(b) and (c) in criminal cases and bankruptcy cases.

None.

Respectfully submitted,

Dated: March 20, 2023

By: /s/ James Hannah

Paul J. Andre  
James Hannah  
Kramer Levin Naftalis & Frankel LLP  
333 Twin Dolphin Drive, Suite 700  
Redwood Shore, CA 94065  
Tel: (650) 752-1700  
Fax: (650) 752-1800  
pandre@kramerlevin.com  
jhannah@kramerlevin.com

Jeffrey H. Price  
Kramer Levin Naftalis & Frankel LLP  
1177 Avenue of the Americas  
New York, NY 10036  
Tel: 212.715.7502  
Fax: 212.715.8302  
jprice@kramerlevin.com

*Attorneys for Appellant*  
CUPP Computing AS

## **TABLE OF CONTENTS**

	<b>Page</b>
STATEMENT OF RELATED CASES .....	1
JURISDICTION.....	3
STATEMENT OF THE ISSUES.....	4
INTRODUCTION .....	5
STATEMENT OF THE CASE AND FACTS .....	7
I.    BACKGROUND OF THE TECHNOLOGY .....	7
A.    Mobile Security.....	7
B.    The '344 Patent .....	9
II.   THE IPR PROCEEDING.....	11
A.    The Groenendaal Reference.....	11
B.    The Parties' Arguments and the Board's Findings Regarding the "configured to be processed" Limitation (Claims 19 and 20).....	15
C.    The Parties' Arguments and the Board's Findings With Respect to the "configured to mirror" Limitation (Dependent Claims 8 and 17) .....	23
SUMMARY OF THE ARGUMENT .....	25
ARGUMENT .....	28
I.    STANDARD OF REVIEW .....	28
II.   THE COURT SHOULD REVERSE THE BOARD'S CONCLUSION THAT CLAIMS 19 AND 20 ARE OBVIOUS .....	29

A.	The Board Failed to Construe “Configured to Be Processed” Before Determining Obviousness .....	30
B.	The FWD is Based Only on Conclusory Expert Testimony and Ignored CUPP’s Evidence, in Violation of the APA and CUPP’s Due Process Rights .....	32
1.	The FWD is Supported Solely by Conclusory Expert Testimony.....	34
2.	The Board’s Failure to Consider CUPP’s Rebuttal Evidence and Arguments Violated Due Process and the APA.....	36
III.	THE COURT SHOULD REVERSE THE BOARD’S CONCLUSION THAT CLAIMS 8 AND 17 ARE OBVIOUS .....	40
A.	The Board’s Reliance on New Arguments at Oral Argument Violated the APA and CUPP’s Due Process Rights.....	41
B.	The Board Failed to Consider the Order of Operations that the Claims Require .....	42
	CONCLUSION .....	45

## TABLE OF AUTHORITIES

	<b>Page(s)</b>
<b>Cases</b>	
<i>Abbott Labs. v. Cordis Corp.</i> , 710 F.3d 1318 (Fed. Cir. 2013) .....	36
<i>Banyan Licensing, L.C. v. Orthosupport Intern., Inc.</i> , 34 F. App'x 696 (Fed. Cir. 2002) .....	43
<i>Belden Inc. v. Berk-Tek LLC</i> , 805 F.3d 1064 (Fed. Cir. 2015) .....	36
<i>Chef Am., Inc. v. Lamb Weston, Inc.</i> , 358 F.3d 1371 (Fed. Cir. 2004) .....	43
<i>CUPP Computing AS v. Trend Micro Inc.</i> , No. 20-2059, 2022 WL 5239075 (Fed. Cir. Oct. 6, 2022) .....	16
<i>Dell Inc. v. Acceleron, LLC</i> , 818 F.3d 1293 (Fed. Cir. 2016) .....	41
<i>Function Media, L.L.C. v. Google, Inc.</i> , 708 F.3d 1310 (Fed. Cir. 2013) .....	43
<i>In re Hodges</i> , 882 F.3d 1107 (Fed. Cir. 2018) .....	29
<i>Homeland Housewares, LLC v. Whirlpool Corp.</i> , 865 F.3d 1372 (Fed. Cir. 2017) .....	31, 32
<i>In re Kahn</i> , 441 F.3d 977 (Fed. Cir. 2006) .....	34
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	34
<i>In re Lee</i> , 277 F.3d 1338 (Fed. Cir. 2002) .....	34
<i>Mformation Techs., Inc. v. Research in Motion Ltd.</i> , 764 F.3d 1392 (Fed. Cir. 2014) .....	43
<i>In re Nuvasive, Inc.</i> , 842 F.3d 1376 (Fed. Cir. 2016) .....	36, 37

<i>Owens Corning v. Fast Felt Corp.</i> , 873 F.3d 896 (Fed. Cir. 2017) .....	45
<i>Pers. Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017) .....	28, 29
<i>Personalized Media Commc'ns, LLC v. Apple Inc.</i> , 952 F.3d 1336 (Fed. Cir. 2020) .....	28
<i>Power Integrations, Inc. v. Lee</i> , 797 F.3d 1318 (Fed. Cir. 2015) .....	38
<i>Qualcomm Inc. v. Intel Corp.</i> , 6 F.4th 1256 (Fed. Cir. 2021) .....	41
<i>TI Grp. Auto. Sys. (N. Am.), Inc. v. VDO N. Am., L.L.C.</i> , 375 F.3d 1126 (Fed. Cir. 2004) .....	30
<i>TQ Delta, LLC v. Cisco Sys., Inc.</i> , 942 F. 3d 1352 (Fed. Cir. 2019) .....	34, 35, 38
<b>Statutes</b>	
5 U.S.C. § 706(2)(A), (E) .....	29
28 U.S.C. § 1295(a)(4)(A) .....	3
35 U.S.C § 282(b). .....	28
35 U.S.C. § 103 .....	5, 11
Administrative Procedure Act.....	<i>passim</i>
<b>Other Authorities</b>	
37 C.F.R. § 42.100(b) .....	28
37 C.F.R. § 42.104(b)(4).....	19

### **STATEMENT OF RELATED CASES**

Pursuant to Federal Circuit Rule 47.5, CUPP Computing AS states that:

(1) CUPP previously filed the following appeal:

- *CUPP Computing AS v. Trend Micro Inc.*, No. 20-2059 (Fed. Cir. Oct. 6, 2022)<sup>1</sup>. The decision was issued on October 6, 2022 before the panel of Circuit Judges Dyk, Taranto, and Stark, and it was not published in the Federal Reporter.

Other than the above listed matter, no appeal other than the current appeal has been taken in or from the United States Patent and Trademark Office, Patent Trial and Appeal Board's decision in No. IPR2021-00813.

(2) CUPP Computing AS and Trend Micro, Inc., are parties to *CUPP Cybersecurity, LLC v. Trend Micro, Inc.*, No. 3:18-cv-01251 (N.D. Tex.) (consolidated with 3:20-cv-03206 (N.D. Tex.)); *CUPP Cybersecurity LLC v. Symantec Corp.*, 3:19-cv-00298 (N.D. Cal.).

---

<sup>1</sup> CUPP appealed the Board's Final Written Decision regarding U.S. Patent No. 9,781,164 (the "'164 Patent") to the Federal Circuit. The '344 Patent is a continuation of the '164 Patent, and shares a common specification with the '164 Patent.

(3) no other cases may directly affect or be directly affected by this Court's decision in this appeal.

### **JURISDICTION**

The Patent Trial and Appeal Board (the “Board”) issued on October 14, 2022, Final Written Decision in IPR2021-00813 (“the FWD”). Appx1-41. Patent Owner, CUPP Computing AS (“CUPP”), timely filed Notice of Appeal on November 3, 2022. Appx536-540. This Court has jurisdiction over this appeal pursuant to 28 U.S.C. § 1295(a)(4)(A).

### **STATEMENT OF THE ISSUES**

1. Whether the Board erred relying solely on conclusory expert testimony to find that Groenendaal discloses the “configured to be processed” limitation.
2. Whether the Board violated the Administrative Procedure Act (“APA”) and due process by failing to consider CUPP’s rebuttal arguments and evidence in finding that the “configured to be processed” limitation is found in the prior art.
3. Whether the Board violated the APA and due process by basing its construction of the term “configured to be mirrored” on an argument made for the first time during the Oral Hearing.
4. Whether the Board erred in rewriting the term “the security code, the security policy, and the security data are configured to mirror security policies of a gateway” to state that a gateway is configured to mirror security policies of the security system, rather than—as the text says—that a security system is configured to mirror security policies of a gateway.

## **INTRODUCTION**

The Board's FWD invalidated Claims 8, 17, 19, and 20 of U.S. Patent No. 10,621,344 ("the '344 Patent") as obvious under 35 U.S.C. § 103 in view of U.S. Patent Publ. No. 2005/0260996 to Groenendaal. This decision should be reversed because the Board failed to engage in the required two-step process of construing key claim terms before evaluating patentability. As a result, the Board violated due process and the APA by disregarding CUPP's rebuttal arguments and evidence, relying on conclusory opinions, and unsupported claim construction positions raised for the first time at oral argument.

With respect to the "configured to be processed" limitation of Claims 19 and 20, the Board engaged in a circular approach that resulted in reversible error. As an initial matter, the Board failed to construe key claim terms before conducting its obviousness analysis, reasoning that no construction was necessary because, even under CUPP's proposed construction, the prior art taught the "configured to be processed" limitation. Appx22-23. Yet at the same time, the Board refused to consider CUPP's arguments and evidence that showed the prior art lacked the limitation under this construction, on the illogical basis that it had "rejected" this very construction that it was purporting to apply. This inconsistent rationale compounded the error in the Board's failure to construe the limitation in the first

place. The Board then erroneously credited the conclusory opinion of Trend Micro's expert to make the untenable finding that the prior art disclosed the limitation.

With respect to the "configured to mirror" limitation of Claims 7 and 18, the Board deprived CUPP of due process by relying on a claim construction argument raised for the first time during the Oral Hearing. The Board used this argument in rewriting the limitation to encompass exactly the opposite of what CUPP claimed. If the limitation is properly construed just as it is written, there is no dispute that the prior art does not satisfy it.

For these reasons, as explained further below, the Court should reverse the Board's obviousness findings.

## **STATEMENT OF THE CASE AND FACTS**

This appeal is taken from *inter partes* review (“IPR”) of the ’344 Patent in IPR2021-00813. Appellant CUPP Computing AS (“CUPP”) appeals the Board’s rulings that Claims 8, 17, 19, and 20 of the ’344 Patent are unpatentable, including the Board’s construction of the limitations “configured to be processed by the security system processor to implement security services for a mobile device” and “configured to mirror,” as well as the Board’s obviousness conclusions.

### **I. BACKGROUND OF THE TECHNOLOGY**

#### **A. Mobile Security**

Traditional enterprise network systems employ two lines of defense to protect users from malicious code received over the internet, such as viruses, spyware, adware, worms, and trojan horses. Appx64 at 1:49-2:2. The first line of defense is provided by the enterprise network’s security system, which sits at or near the boundary of a network and protects all devices located on the network. *Id.* at 1:63-66. The second line of defense is provided by security applications installed on individual devices, whether inside or outside of the trusted enterprise network. *Id.* at 1:66-2:2.

As mobile devices began to proliferate in the early 2000s, mobile device security became increasingly important because such devices did not enjoy the same level of security outside of an enterprise network as would be provided by the

enterprise network's security system. *Id.* at 2:45-52. In particular, mobile devices traveling outside of the trusted enterprise network lose the first line of defense and become more susceptible to attacks. Figure 2 of the '344 Patent, reproduced below, shows a traditional network system architecture in which a mobile device has traveled outside the trusted enterprise and is no longer protected by network security system 120, which provides the first line of defense to devices on the network, like desktop 105:

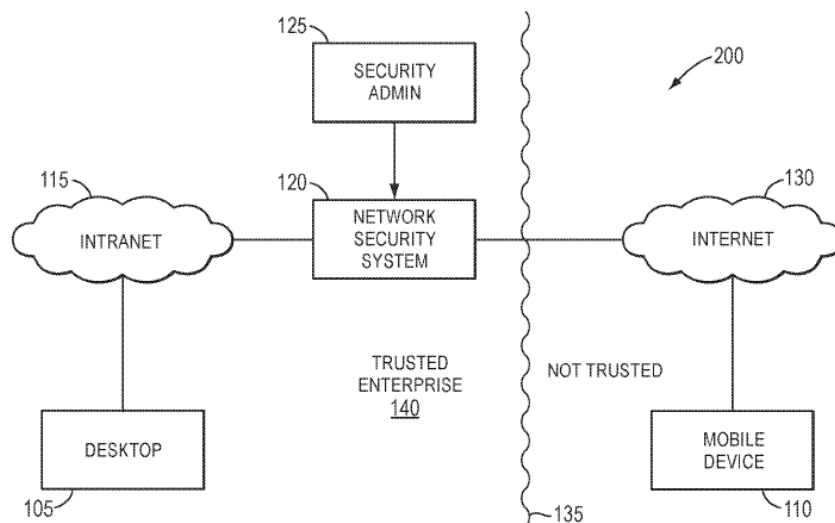


FIG. 2  
(PRIOR ART)

Appx55 at FIG. 2. This loss of security is problematic not only for the mobile device but also for the trusted enterprise network. Specifically, the mobile device risks transferring any malicious code to the trusted enterprise if the code travels back into the trusted enterprise and reconnects to it. Appx64 at 2:31-44. Accordingly, a need

arose for a mobile security system that, by paralleling the enterprise network security system, maintains the first line of defense even when the mobile device travels outside the trusted network. *Id.* at 2:45-52.

## **B. The '344 Patent**

The '344 Patent met this need by describing and claiming a security system that processes security code, security policies, and security data (“security information”) in order to implement security services for a mobile device. Appx66 at 5:27-39, Appx66-67 at 5:61-7:48, Appx67-68 at 8:42-9:8, Appx58 at FIG. 5, Appx61 at FIG. 7. As described and claimed, the security system stores the security information in memory, and the security system’s processor processes the security information to implement security services on behalf of the mobile device. The implemented security services might consist of, for example, a firewall, an intrusion detection system (“IDS”), an intrusion prevention system (“IPS”), or antivirus/malicious content detection. *See* Appx66 at 6:23-50 (listing the software packages that may be implemented “on the mobile security system”), Appx69 at 12:25-28 (security engines, such as firewall, antivirus, and IPS/IDS engines, are loaded “on the mobile security system”); *see also* Appx66-67 at 6:5-7:3, Appx67 at 7:31-48, Appx57-58 at FIGs. 4, 5 (detailing the hardware of the mobile security system).

As illustrated in Figure 3, reproduced below, the '344 Patent discloses a security system that acts as a mobile internet gateway for mobile devices traveling outside of the trusted enterprise network. By processing security information to implement security services for the mobile device, this architecture keeps the first line of defense intact even when the mobile device leaves the trusted enterprise network:

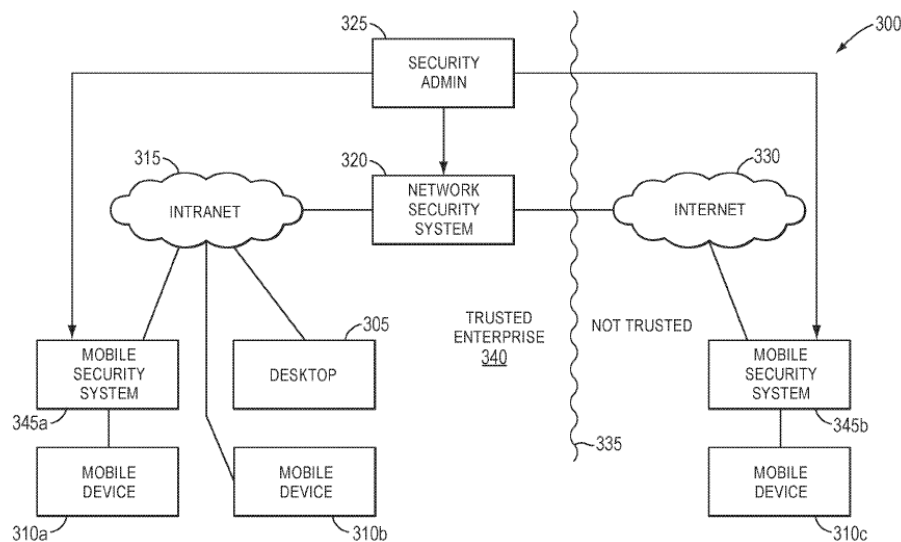


FIG. 3

Appx56 at FIG. 3; Appx65-66 at 4:57-5:34.

In one embodiment, recited in Claims 8 and 17, the security information stored on the security system is “configured to mirror security policies of a gateway on the trusted enterprise network.” Appx71-72. This technique achieves the '344 Patent's stated goal of ensuring that “the mobile device 310 *c* currently traveling may have the same level of protection as the devices 305/310 within the trusted enterprise.”

Appx66 at 5:55-60; *see also* Appx50 at Abstract (“Using the piece of hardware, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.”); Appx64 at 2:60-63. The specification discloses achieving this goal by translating the enterprise’s security policies into mobile security policies and configuring the mobile security system to implement these translated policies. Appx66 at 5:50-55.

## **II. THE IPR PROCEEDING**

The Petition challenged Claims 1-20 of the ’344 Patent as obvious under 35 U.S.C. § 103 in view of U.S. Patent Publ. No. 2005/0260996 to Groenendaal. Appx81. This appeal concerns the Board’s findings with respect to Claims 8, 17, 19, and 20.

### **A. The Groenendaal Reference**

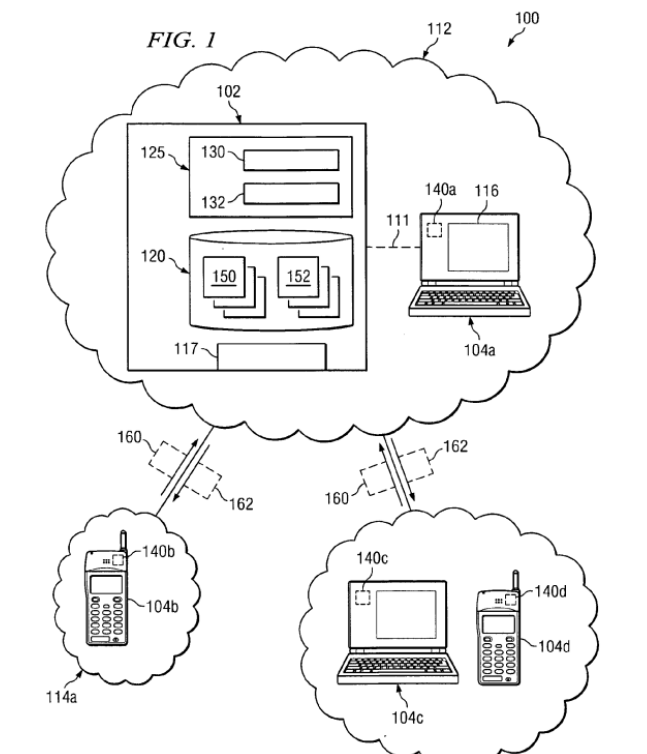
Groenendaal discloses securing an enterprise network by either (1) enforcing security policies directly on an agent executing on the mobile device or (2) configuring infrastructure entities to enforce the security policies within the enterprise network:

[A] firewall policy for a given user can be configured or implemented on a wireless gateway when the user enters a particular access-zone, or if the particular mobile device is running an agent, the policy might be enforced via the agent.

Appx739-740 at ¶ 14; *see also* Appx745 at ¶ 31 (enterprise network 112 includes a security gateway that has been pushed policies for enforcement). Just like traditional

network systems, Groenendaal's system employs the mobile device itself, or an infrastructure entity within the enterprise network, to process security policies. Groenendaal does not leverage its server (the alleged security system)<sup>2</sup> to perform these actions.

Groenendaal discloses that server 102 of the enterprise network 112 (shown in Figure 1 reproduced below) executes a security manager 130 that provides a security profile or configuration profile to an agent of the mobile device or a gateway of the enterprise network, which then implements that profile:



<sup>2</sup> Trend Micro maps Groenendaal’s server 102 to the claimed “security system.” See Appx96 (“Groenendaal discloses that server 102 (security system) . . .”); see also *infra* a table of Trend Micro’s mappings.

Appx722 at FIG. 1; Appx744-745 at ¶ 29 (“Client 104 also includes references, or executes agent 140. Agent 140 . . . implements a security end-point in the wireless network by implementing associated security profiles 150 and/or configuration profiles 152.”); Appx745 at ¶ 31 (“In the case that enterprise 112 includes a security gateway (e.g., Bluesocket), security manager 130 may push policies (e.g., access zone policies, access point policies, firewall policies) to the security gateway for enforcement.”). Thus, instead of server 102 processing security information to implement security services for the mobile device, Groenendaal discloses managing the security of mobile devices by choosing a security profile and transmitting the chosen profile to the mobile device or gateway for enforcement. Appx739-740 at ¶ 14.

Groenendaal’s “additional security services” are also processed and enforced on the mobile device or gateway. *See* Appx343-344 (listing “additional security services” as “commanding clients to perform actions, and configuring infrastructure entities such as wireless gateways”). With respect to “commanding clients,” the mobile device actually “execute[s] the command” such that “the processing happens on the mobile device.” Appx517-518 at 46:21-47:7. Turning to “configuring infrastructure entities,” this procedure involves nothing more than sending security and configuration profiles to the gateway for processing and implementation of the security policy, *e.g.*, firewall. *See* Appx517 at 46:2-6 (“Sure, the server may not

implement a firewall itself.”), Appx518 at 47:20-24 (the wireless gateway implements the security policies based on the security and configuration profiles).

Accordingly, in Groenendaal’s system, either the agent of the mobile device or a gateway within the enterprise network processes the relevant profiles and implements the security services. Appx739-740 at ¶ 14, Appx744-745 at ¶ 29, Appx745 at ¶ 31. Critically, Groenendaal does not teach, and the Board did not find, that server 102’s alleged security services are implemented for the mobile device as a result of processing the claimed security information. At best, server 102 simply provides profiles to a mobile device or an infrastructure entity. It is the mobile device or infrastructure entity that then processes the chosen policy.

The table below shows Trend Micro’s mapping of Groenendaal’s features to several key claim elements:

<b>Claim Elements</b>	<b>Cited Groenendaal Features</b>
a trusted enterprise network	enterprise network 112
a security system	server 102 of the enterprise network 112
a security system processor	server 102’s processor 125
security information <sup>3</sup>	security profiles 150 and configuration profiles 152 (“profiles”)
[security information] configured to be processed by the processor [of the security system] to implement security services for a mobile device	-commanding the mobile device to perform an action (e.g., block port 80) -configuring infrastructure entities to enforce security policies (e.g., firewall)

---

<sup>3</sup> For brevity, “at least a portion of security code, at least a portion of a security policy, and at least a portion of security data” is collectively referred to as “security information.”

Claim Elements	Cited Groenendaal Features
security system's security information is configured to mirror the security policies of a gateway on the trusted enterprise network	Server 102 pushes policies to the security gateway for enforcement

*See generally* Appx71-73 (Claims 8, 17, 19, and 20); Appx89, Appx97-98, Appx104-105, Appx128-129 (Petition).

The point at the heart of this dispute is that server 102 does not process the alleged security information to implement security services for a mobile device. Instead, it simply *pushes* information to *other* devices for processing and implementation. Trend Micro admits this. Appx517-518 at 46:4-47:8 (conceding that server 102 does not process and implement a firewall itself nor block port 80).

Nor is this security information configured to mirror the policies of a gateway on the trusted enterprise network. Instead, Groenendaal's security and configuration profiles are defined on server 102 and sent to the mobile device or gateway for processing.

**B. The Parties' Arguments and the Board's Findings Regarding the "configured to be processed" Limitation (Claims 19 and 20)**

In the Petition, Trend Micro proposed a construction for the phrase "implement security services for a mobile device," which is recited in Claims 19 and 20 of the '344 Patent. Appx86 ("implement[ing] security services for a mobile device" requires nothing more than carrying out or accomplishing the act of sending

security information to the mobile device). Reasoning that the Board in an earlier proceeding concerning a related patent had already construed the phrase “provide security services to a mobile device”—which appears in Claim 1 (Limitation 1.4)—to include the act of sending security information to the mobile device,<sup>4</sup> Trend Micro argued that “implement[ing] security services for a mobile device” requires nothing more than carrying out or accomplishing the act of sending security information to the mobile device. Appx86. Trend Micro also argued that Groenendaal’s server 102 can perform additional security services, such as “configuring infrastructure entities,” (*id.*) which presumably would meet a narrower yet unspecified construction of this term. Appx104-105.

Trend Micro then concluded, with no reference to any objective construction of the claim or citation to record evidence, that the act of configuring another device, like a gateway, to enforce a security policy involves “the security system processor [] processing the stored security code, security policies, and security data, as established for limitation 1.4.” *Id.* The plain language of Limitation 1.4, however, does not require that the security information be processed *by the security system processor*. Furthermore, Trend Micro did not argue that any of the alleged security

---

<sup>4</sup> Appx787-790 (the ’164 Final Written Decision). This Court affirmed the Board’s construction. *See CUPP Computing AS v. Trend Micro Inc.*, No. 20-2059, 2022 WL 5239075 (Fed. Cir. Oct. 6, 2022).

services are implemented through processing of any security policies or data *by the security system processor*. See Appx100-104.

In response to Trend Micro’s position, CUPP addressed the meaning of the term “implement security services for a mobile device,” in isolation, as well as the meaning of the full phrase, *i.e.* security information “*configured to be processed by the security system processor to implement security services for a mobile device.*” CUPP raised separate arguments for each phrase, and each represented an independent basis to reject Trend Micro’s position. Appx286-292.

With respect to the isolated “implemented” phrase, CUPP argued that the term “implement security services for a mobile device,” recited in Claims 19 and 20, distinguished these claims from Independent Claims 1 and 10, which broadly recite that the security system must only “provide security services to a mobile device.” Appx287-292. CUPP argued that the term used in Claims 19 and 20 specifically refers to those embodiments of the ’344 Patent where the security system “*implements*” security services on behalf of a mobile device, such as by executing a security policy to establish a firewall, rather than merely *configuring* the mobile device to implement the security services *itself*. Appx289-292.

Aside from the difference in the plain language of the claims, CUPP’s expert, Dr. Goodrich, showed that Trend Micro’s construction lacked intrinsic support because it conflates “sending security information to a *security system* with sending

security information to a *mobile device*.” Appx290 (quoting Appx1399-1400 at ¶ 54). Dr. Goodrich, therefore, showed that the intrinsic evidence supported CUPP’s construction of the isolated “implementing” phrase, which requires that *the security system processor* implement security services *for* the mobile device, and not Trend Micro’s construction, in which the security services are implemented on the mobile device *itself*. Appx300-307 (citing Appx1414-1424 at ¶¶ 85-102).

Dr. Goodrich also cited numerous examples from the specification illustrating the various ways that the claimed security system can and does process security code, security data, and security policies to implement security services for a connected mobile device, as claimed. Appx1397-1398 at ¶¶ 50-51. For example, the security system processor can process such security information to implement a firewall, VPN, IDS/IPS protection, and/or perform malicious content detection for, or on behalf of, the mobile device. *See* Appx66 at 6:23-50. In these claimed embodiments, and in concert with the goal of the invention, the security system’s implementation of security services retains the first line of defense for the mobile device when the device travels outside the trusted enterprise network. Appx276-277.

CUPP’s main argument, however, related to the full claim limitation, which requires that the security information is “*configured to be processed by the security system processor to* implement security services for a mobile device.” Appx286-

292 (emphasis added). CUPP argued that this limitation requires that “the processing of the security information *results* in the implementation of the security services for the mobile device.” Appx287 (citing Appx1397 at ¶ 49). Dr. Goodrich’s opinion about the scope of this limitation was based primarily on the plain language of the claims, which literally require that the security system process security information “to implement security services for the mobile device.” Appx1414 at ¶ 86; Appx72-73 (Claims 19 and 20).

Based on this plain-language reading of Claims 19 and 20, CUPP observed that none of the “security services” that Groenendaal’s server allegedly provides to the mobile device result from having the security system process the claimed security information. Appx287-289, Appx301-307. In fact, CUPP addressed every alleged “security service” cited in the Petition and, supported by the underlying evidence as analyzed and interpreted by Dr. Goodrich, concluded that each exemplary security service is implemented by having the mobile device (or gateway)—not the security system—process the alleged security information. Appx301-307 (citing Appx1414-1424 at ¶¶ 85-102). CUPP further observed that “Petitioner has not pointed out what disclosures in *Groenendaal* allegedly correspond to the security policy, code, and data *processed by the security system*,” as required under 37 C.F.R. § 42.104(b)(4). Appx305; *see also* Appx376-377. Indeed, Trend Micro’s expert’s (Dr. Jakobsson’s) conclusion on this point referred

back to an earlier analysis that *did not* tie the alleged security services to *the security system's processing* of any security policies or data. Appx1207-1208 at ¶¶ 101-106.

Trend Micro's Reply neither challenged nor rebutted Dr. Goodrich's testimony that the full claim term requires that *the security system* implement the claimed security services as a result of *processing* the claimed security information. Appx1397-1399 at ¶¶ 49-52. In fact, Trend Micro acknowledged that CUPP's proposed construction "is redundant to the claim language." Appx328. Without any further discussion of the full limitation, Trend Micro proceeded to address in CUPP's arguments regarding the scope of phrase "implement security services for a mobile device" in isolation. *See* Appx328-332.

Rather than dispute the substance of CUPP's proposed construction for the full "configured to be processed" limitation, Trend Micro argued for the first time in its Reply that "the Groenendaal server processes the stored security policies, data, and code because it must determine how to configure an infrastructure entity, which infrastructure entity to configure, and when." Appx344-345. This argument in the Reply does not appear in the cited portion of the Petition, does not cite any underlying factual or testimonial evidence, and does not explain how this determination involves the security system processor processing any security policies or security data. *See* Appx100-105 (concerning Limitation 1.4, which does not include the "configured to be processed" limitation). Nor does this argument

rebut or address any of Dr. Goodrich's testimony on this issue or introduce cross-examination or rebuttal evidence calling his analysis into doubt. *See* Appx328-332, Appx340-347.

In its Sur-Reply, CUPP reminded the Board that Dr. Goodrich's undisputed testimony, and the underlying evidence in Groenendaal itself, already addressed Trend Micro's new attorney argument regarding determining how and when to configure an infrastructure entity to enforce a security policy. Appx374-376 (showing that the "tailoring security profiles and sending profiles to an access point" involves nothing more than defining and transferring the profile to the access point or mobile device). In fact, the Board previously determined, and this Court recently confirmed, that those determinations are made in the mind of an IT administrator, not by the security system processor processing any security policies or security data. Appx810 ("Groenendaal's IT administrator's policies, by contrast, are the IT administrator's decisions about rules about security, which the IT administrator uses to provide appropriate input to GUI 116 in order to implement those policies on client computers 104.") (citation omitted).

At the Oral Hearing, Trend Micro conceded that Groenendaal's server 102 does not process the security and configuration profiles to implement security services for the mobile device. Appx517-518 at 46:4-6-47:24 ("Sure, the server may not implement a firewall itself . . ." instead "infrastructure entities [] enforce security

policies [e.g., firewall]”); *id.* at 46:21-47:7 (“It’s true. The mobile device would execute the command . . . block port 80” and “[s]o the processing . . . happens on the mobile device.”). Yet the Board in its FWD found that Trend Micro had met its burden to show that Groenendaal teaches this claim element. *See* Appx31. It did so despite Trend Micro’s concession, Trend Micro’s failure to point out which specific security policies and data are allegedly processed *at the security system* to implement security services for the mobile device, and Dr. Goodrich’s un rebutted and unchallenged testimony that the configuring of an infrastructure device or mobile device involves nothing more than sending the relevant security and configuration profiles to the device.

In its FWD, the Board began its analysis by considering the parties’ arguments regarding the meaning of “implement security services for a mobile device” in isolation. Appx20-22. Although the Board stated that it disagreed with CUPP’s arguments regarding the meaning of the term in isolation, it never analyzed CUPP’s primary claim construction argument, *i.e.* that the full limitation requires that “the processing of the security information results in the implementation of the security services for the mobile device.” Appx1397 at ¶ 49.

Rather than construe the full term, the Board stated that no construction was necessary because it determined that Groenendaal disclosed the “configured to be processed” limitation even under CUPP’s proposed construction, citing only Dr.

Jakobsson’s conclusory assertion that each of Groenendaal’s “additional” services is “implemented by the security server processor by processing the stored security code, security policies, and security data, as established for [L]imitation 1.4.” *See* Appx22 (quoting App1208 at ¶ 105). Incredibly, however, in the portion of the FWD where the Board purportedly applied CUPP’s proposed construction, it explicitly stated that it gave no weight to Dr. Goodrich’s extensive, uncontested rebuttal testimony, and CUPP’s arguments relying thereon, on the basis that it *disagreed* with CUPP’s claim construction argument. Appx34. Thus, the Board’s analysis was entirely circular, and, as a result, the Board failed to determine the proper scope of the full “configured to be processed” limitation and to evaluate the parties’ arguments under the undisputed plain-language interpretation.

**C. The Parties’ Arguments and the Board’s Findings With Respect to the “configured to mirror” Limitation (Dependent Claims 8 and 17)**

The Board also adopted Trend Micro’s flawed argument with respect to the “configured to mirror” limitation of dependent Claims 8 and 17. These claims each recite, in relevant part:

wherein the security code, the security policy, and the security data are configured to mirror security policies of a gateway on the trusted enterprise network

Appx71-72 (Claims 8, 17). Accordingly, the security information of the security system is “configured to mirror” the security policies of the gateway on the trusted enterprise network.

In its Petition, Trend Micro asserted that Groenendaal meets the “configured to mirror” limitation because the policies on server 102 mirror those on the gateway, even though Groenendaal teaches just the opposite. Appx129-130. Trend Micro argued that Groenendaal satisfies the limitation because, after the policies are pushed from server 102 to the gateway, the policies of server 102 would match the policies on the gateway. Appx130 (“When these policies are pushed [from server 102] to the security gateway, they would match the same security policies stored on server 102.”); *see also* Appx350-351.

In response, CUPP showed that Trend Micro’s allegation was illogical because the policies on Groenendaal’s gateway are configured to mirror those of the server, not the other way around, because the gateway’s policies are configured when server 102 pushes its policies onto the gateway. Appx310-312; Appx379-381. These policies exist first on server 102 and are then pushed to the gateway meaning that if any policy is configured to mirror another, the gateway’s policy mirror’s the servers, not the other way around, as claimed. At the oral hearing, Trend Micro’s counsel for the first time asserted that the claims do not impose an order of operations. Appx493 at 22:20-23.

Relying solely on Petitioner’s remark, made for the first time at the Oral Hearing, the Board determined that the claims do “not impose an order of operations.” Appx39. The Board did not explain how it arrived at this decision, and its analysis does not contain any analysis of the intrinsic evidence, including the claim language itself, which explicitly sets out which policies are configured to mirror which. *Id.* Based only this *sua sponte* interpretation, the Board found that Groenendaal meets the claims because, after the gateway’s security policies are configured, the server’s policies match. *Id.*

### **SUMMARY OF THE ARGUMENT**

The FWD should be reversed because the sole prior art reference cited against the claims does not disclose a security system that processes security information in order to implement security services for a connected mobile device, as recited in Independent Claims 19 and 20, or configuring such security information to mirror security policies of a gateway on the trusted enterprise network, as recited in dependent Claims 8 and 17, as those terms are properly understood.

With respect to the “configured to be processed” limitation, the lion’s share of the Board’s analysis considered whether the term “implement security services for a mobile device,” in isolation, encompasses the act of sending security information to another device. Appx16-17, Appx20-22. The Board devoted only one paragraph of the FWD considering CUPP’s arguments about the meaning of this

term in its full context, which requires that the security system implement these security services as a result of processing security code, a security policy, and security data. Appx22.

Ultimately, the Board declined to construe the term, determining that the issue was moot in view of its later analysis of the parties' arguments under CUPP's construction. Appx22-23. Then, the Board accorded no weight to entire swaths of Dr. Goodrich's unchallenged, unrebutted, and detailed rebuttal of Dr. Jakobsson's conclusory testimony, stating that it had "rejected" that very construction. Appx34. The Board's analysis, therefore, was entirely circular: It declined to construe a key claim term because it credited Dr. Jakobsson's conclusory testimony that the limitation was met and declined to consider Dr. Goodrich's detailed rebuttal of that conclusion on the basis that it rejected CUPP's construction. Appx22; Appx34. Furthermore, the Board adopted Dr. Jakobsson's conclusory testimony without evaluating the evidence underlying the conclusion or even identifying which, if any, security services are implemented as a result of the security system processing the claimed security information. *Id.*

The Board's approach here is reversible according to this Court's precedent, which requires that the claims be construed before determining obviousness, holds that the Board violates the APA when it does not give a patent owner the opportunity to be heard, and forbids an obviousness determination supported only by conclusory

expert testimony. Each one of those errors requires reversal because the only possible finding that can be drawn from the Groenendaal reference under the proper construction is that there are no security services “implemented” as a result of *the security system* processing security policies and security data.

With respect to the “configured to mirror” limitation, the Board rewrote the claims to encompass the opposite of what the claims recite. As claimed, this limitation requires that the security system’s security information be “configured to mirror security policies of a gateway on the trusted enterprise network.” Groenendaal undisputedly discloses the opposite: In Groenendaal, the “gateway” receives and implements security policies received from the alleged “security system.” Appx39. In order to sweep the prior art’s disclosure into the claims, the Board relied on Trend Micro’s argument, made for the first time during the Oral Hearing, that “claims 8 and 17 do not impose an order of operations . . . . After one has configured a server and a gateway to have the same policies they are configured to mirror each other.” *Id.* The Board’s reliance on this new argument violates this Court’s precedent and the APA. It also rewrites the plain language of the claims to remove the requirement that the security system’s security information be configured to mirror the security policies of the gateway, and not vice versa. Because there is no dispute that Groenendaal does not disclose this limitation as

properly construed, this Court should reverse the Board’s obviousness determination with respect to Claims 8 and 17.

## **ARGUMENT**

### **I. STANDARD OF REVIEW**

**Claim Construction:** This Court reviews “de novo the Board’s ultimate claim constructions and any supporting determinations based on intrinsic evidence.” *Personalized Media Commc’ns, LLC v. Apple Inc.*, 952 F.3d 1336, 1339 (Fed. Cir. 2020) (citation omitted). While reviewing “any subsidiary factual findings involving extrinsic evidence for substantial evidence.” *Id* (citation omitted). “In an *inter partes* review proceeding, a claim of a patent . . . shall be construed using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b).

**Obviousness:** This Court reviews “the Board’s ultimate determination of obviousness de novo and its underlying factual determinations for substantial evidence.” *Pers. Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 991 (Fed. Cir. 2017) (citation omitted).

**The Board's Compliance with the Administrative Procedure Act:** This Court reviews “the Board’s IPR decisions to ensure that they are not ‘arbitrary, capricious, an abuse of discretion, . . . otherwise not in accordance with law . . . [or] unsupported by substantial evidence.’” *Pers. Web Techs.*, 848 F.3d at 992 (quoting 5 U.S.C. § 706(2)(A), (E)) (further citation omitted).

## **II. THE COURT SHOULD REVERSE THE BOARD’S CONCLUSION THAT CLAIMS 19 AND 20 ARE OBVIOUS**

This Court should reverse the Board’s conclusion that Claims 19 and 20 are obvious because the Board’s findings based on the “configured to be processed” limitation were in error. Rather than construing the term and then determining whether the claims were valid under the correct construction, the Board purported to apply CUPP’s proposed construction in its obviousness analysis. Appx22. However, when purporting to apply CUPP’s construction—which Trend Micro acknowledged was “redundant” to the claim language, or in other words *precisely what the language of the claim says*—the Board credited Dr. Jakobsson’s conclusory assertion that the limitation was met and explicitly declined to consider CUPP’s rebuttal evidence and arguments. Appx34. Under the proper construction, which the parties did not dispute, the Board’s obviousness determination contravenes the only permissible findings that can be drawn from *Groenendaal*. *In re Hodges*, 882 F.3d 1107, 1115-17 (Fed. Cir. 2018) (reversing the Board’s anticipation findings

because they “contravene the only permissible findings that can be drawn from the prior art under the proper constructions of the relevant claim terms”).

**A. The Board Failed to Construe “Configured to Be Processed” Before Determining Obviousness**

The Board’s FWD should be reversed because it declined to determine a key claim construction issue—namely, whether the “configured to be processed” term requires that the security services implemented by the security system must result from the processing of security information stored in the security system’s memory—before considering the parties’ validity arguments that depended on this determination.

This Court’s precedent requires that every validity analysis begins with determining the proper scope of the claims. Only after properly construing the claims may the Board move on to determining whether the properly construed claims are valid. *TI Grp. Auto. Sys. (N. Am.), Inc. v. VDO N. Am., L.L.C.*, 375 F.3d 1126, 1139 (Fed. Cir. 2004) (“Our validity analysis is a two-step procedure: The first step involves the proper interpretation of the claims. The second step involves determining whether the limitations of the claims as properly interpreted are met by the prior art.”) (citation and internal quotation marks omitted). With respect to the “configured to be processed” limitation, the Board collapsed these two steps into one. *See* Appx22-23. Rather than determining whether the full “configured to be processed” term should be construed according to the construction proposed in

CUPP’s Response, the Board attempted to moot the issue by relying on its obviousness analysis, allegedly conducted under CUPP’s proposed construction. Appx22 (“Thus, while we agree with Petitioner’s construction, we also agree that Groenendaal meets this limitation under Patent Owner’s construction. *See infra*, Section III.B.5.”).

Because the Board did not explicitly construe this key claim term, the construction remains one that this Court must resolve. *See Homeland Housewares, LLC v. Whirlpool Corp.*, 865 F.3d 1372, 1375 (Fed. Cir. 2017). However, as made plain in Trend Micro’s Reply, Trend Micro lodged no disagreement with CUPP’s proposed construction of this term. Appx328 (“Patent Owner’s proposed construction therefore is redundant to the claim language and sheds no light on this limitation’s meaning.”). Accordingly, it is undisputed that the plain language of the claims requires that the security services implemented by the security system must result from *the security system* processing security code, security policies, and security data. Appx328.<sup>5</sup>

---

<sup>5</sup> CUPP takes no issue with the Board’s conclusion that Claims 19 and 20 do not “require the security system processor alone to provide services to the mobile device, without the involvement of ‘another infrastructure entity’ such as a gateway.” Appx21-22. These claims do not forbid the implementation of *further* security services downstream of the security system, and the intrinsic record explicitly contemplates more than one line of defense. Appx64 at 1:61-2:44, Appx66 at 5:26-34. Thus, the issue is not whether processing security information at a security system and providing security information to another device are “mutually exclusive

Thus, because the Board did not conduct the two-step analysis required under this Court’s precedent, this Court must construe this claim term. Further, because CUPP’s construction did not rely on any extrinsic evidence, and Trend Micro acknowledged that CUPP’s proposed construction accurately characterizes the “configured to be processed” limitation, the Court should adopt CUPP’s construction, *i.e.* “the security system processes the security information and the processing of the security information results in the implementation of the security services for the mobile device.” Appx287-289; *Homeland Housewares*, 865 F.3d at 1375.

**B. The FWD is Based Only on Conclusory Expert Testimony and Ignored CUPP’s Evidence, in Violation of the APA and CUPP’s Due Process Rights**

The Board engaged in even more flagrant error when it transformed its conclusion that it *need not construe* the “configured to be processed” term into an explicit *disagreement* with CUPP’s construction as part of its obviousness analysis. *Compare* Appx22 (declining to adopt but purporting to apply CUPP’s proposed construction) *with* Appx34 (giving no “weight to Patent Owner’s arguments or the testimony of its expert” because it “rejected” CUPP’s proposed construction). Not

---

activities;” it is whether *any* of Groenendaal’s security services are implemented as a result of processing *by the security system* of all three aspects of the claimed security information. *See* Appx300-307.

only did this disagreement severely magnify the error in the Board’s failure to construe the term in the first place, but it also set the stage for a more serious consequence—a violation of the APA and CUPP’s due process rights.

In collapsing the claim construction and obviousness in this manner, the Board proceeded in a circular path whereby it (1) declined to construe a key claim term, citing its obviousness analysis where it purportedly applied that construction, and (2) declined to consider CUPP’s rebuttal arguments and evidence directed to rebutting Dr. Jakobsson’s testimony and distinguishing Groenendaal on this issue, on the basis that it had “rejected” CUPP’s construction. *See* Appx22 (declining to construe the full “configured to be processed” limitation in view of its later obviousness analysis under CUPP’s construction); Appx34 (declining to consider CUPP’s rebuttal arguments and evidence because it “rejected” CUPP’s construction).

Instead, the Board relied solely on conclusory expert testimony to establish obviousness and refused even to consider CUPP’s extensive rebuttal of Dr. Jakobsson’s conclusory testimony. Appx34 (“We therefore do not give weight to Patent Owner’s arguments or the testimony of its expert, Dr. Goodrich [Appx1412-1427 at ¶¶ 82–107] attempting to rebut Dr. Jakobsson’s testimony or to distinguish Groenendaal.”). The net effect of the Board’s illogical and circular decision-making

deprived CUPP of a fair opportunity to be heard on this issue, thereby violating the APA and CUPP's due process rights.

### **1. The FWD is Supported Solely by Conclusory Expert Testimony**

As an initial matter, the Board erred in crediting Dr. Jakobsson's conclusory testimony about whether Groenendaal discloses a security system that implements security services as a result of processing the claimed security code, policies, and data. Appx34. "[T]he Board is obligated to 'provide an administrative record showing the evidence on which the findings are based, accompanied by the agency's reasoning in reaching its conclusions.'" *TQ Delta, LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1358 (Fed. Cir. 2019) (quoting *In re Lee*, 277 F.3d 1338, 1342 (Fed. Cir. 2002)) (citations omitted). For this reason, the Board's obviousness rejections "cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *Id.* at 1359 (citing *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006))).

The only evidence that the Board cited in its consideration of the relevant aspect of the "configured to be processed" limitation—*i.e.* whether the security services implemented for the mobile device are the result of the security system processing its stored security code, security policy, and security data—is reproduced below:

Each of these services is implemented by the security server processor by processing the stored security code, security policies, and security data, as established for [L]imitation 1.4.

Appx34 (quoting Appx1208 at ¶ 105). This statement does not identify what security code, security policies, or security data are allegedly processed *by the security system* in order to implement the only two services that allegedly meet the full limitation, *i.e.* “‘command[ing]’ the mobile device to perform an action” and “‘configuring infrastructure entities to enforce security policies.” Appx104-105 (Groenendaal’s “additional security services”); Appx343. Nor is there any such explanation in the section of Dr. Jakobsson’s declaration regarding Limitation 1.4. Appx301-304. This is not surprising given that Limitation 1.4 does not require that the security information be processed by the security system processor, in contrast to Limitation 19.4, which specifically requires that *the security code, policies, and data be “configured to be processed to* implement security services for a mobile device.” Appx71-72 (Claims 19, 20).

Because the Board relied only on Dr. Jakobsson’s conclusory testimony on this key contested point, this Court should reverse the Board’s FWD with respect to Claims 19 and 20. *TQ Delta*, 942 F.3d at 1362-63 (reversing a FWD supported only by “conclusory statements and unspecific expert testimony” because it identified no other evidence that could support its conclusion).

## **2. The Board’s Failure to Consider CUPP’s Rebuttal Evidence and Arguments Violated Due Process and the APA**

The Court should reverse the FWD for another reason: The Board’s failure to conduct its obviousness analysis according to the two-part test required by this Court’s precedent violated CUPP’s due process rights and the APA. “The indispensable ingredients of due process are notice and an opportunity to be heard by a disinterested decision-maker.” *Abbott Labs. v. Cordis Corp.*, 710 F.3d 1318, 1328 (Fed. Cir. 2013) (citations omitted). In formal adjudications, like *inter partes* review proceedings, the APA requires that all parties be given the opportunity for “submission and consideration of facts [and] arguments,” including “rebuttal evidence.” *Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1080 (Fed. Cir. 2015) (citations omitted). Further, the “[Board] must provide a reasoned basis for the agency’s action,” and cannot merely “summarize and reject arguments without explaining why the [Board] accepts the prevailing argument.” *In re Nuvasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (citations and internal quotation marks omitted).

In explicitly declining to consider CUPP’s rebuttal arguments and evidence, the Board deprived CUPP of due process and violated the APA. CUPP was not afforded the opportunity to rebut Dr. Jakobsson’s conclusory assertion that each of Groenendaal’s “additional” security services “is implemented by the security server processor by processing the stored security code, security policies, and security data,

as established for [L]imitation 1.4.” Appx34. The Board did not evaluate the arguments made with respect to “limitation 1.4” or identify which security policies code, and data are allegedly processed at the security system to carry out any of the alleged security services. *Id.* The Board did not even attempt to “summarize and reject” CUPP’s rebuttal arguments and evidence, which itself would have fallen short of the consideration the Board must give to a party’s arguments and evidence. *In re Nuvasive*, 842 F.3d at 1383.

The ostensible reason for the Board’s decision to disregard CUPP’s arguments and Dr. Goodrich’s rebuttal testimony and evidence was the Board’s determination that “[t]hose arguments are based on claim constructions and other restrictions *that we have rejected.*” Appx34 (emphasis added). But the Board *had not* rejected CUPP’s proposed construction of the “configured to be processed” term. Rather, it never construed that term and instead stated that it applied *CUPP’s* construction in its obviousness analysis. Appx22. Yet the Board, in turn, explicitly declined to consider CUPP’s rebuttal evidence and arguments distinguishing Groenendaal using this construction on the basis that it *rejected* the very construction that it *purported to apply*. Appx34. The Board’s reasoning, therefore, is illogical and groundless. The Board provided no basis for disregarding evidence and arguments directed to rebutting Dr. Jakobsson’s conclusory assertion that Groenendaal’s server

implements security services as a result of processing the claimed security code, security policy, and security data. *Id.*

CUPP's arguments and evidence were, as the Board admits, made "to rebut Dr. Jakobsson's testimony or to distinguish Groenendaal." *Id.* Specifically, in response to Trend Micro's one-sentence conclusion that Groenendaal's server processes security information to implement security services for a mobile device, Dr. Goodrich devoted eighteen paragraphs of his declaration to painstakingly detail why each of Trend Micro's alleged security services did not result from *the security system* processing the security information, as claimed. Appx1414-1424 at ¶¶ 85-102; *see also* Appx300-307.

Trend Micro did not challenge Dr. Goodrich's testimony or otherwise contest CUPP's arguments on these points. Appx340-346. Instead, Trend Micro introduced entirely new arguments in its Reply about how Groenendaal's server allegedly processes security information. Appx343, Appx346. The Board rightly declined to rely on this new argument in support of its decision, and these new attorney arguments are not subject to review on appeal. *See TQ Delta*, 942 F.3d at 1358 n.4 ("As noted above, our review is limited to 'the grounds upon which the Board actually relied.'" (quoting *Power Integrations, Inc. v. Lee*, 797 F.3d 1318, 1326 (Fed. Cir. 2015) (further citation omitted))).

Indeed, Trend Micro admitted during the Oral Hearing that the only two security services alleged to satisfy Limitation 19.4 in the Petition are not implemented by processing security information at Groenendaal's server. Concerning the first example, Trend Micro conceded that the relevant security services are implemented as a result of processing security and configuration profiles at the mobile device, and implementation of these services, *e.g.*, blocking the port, is also accomplished at the mobile device, not server 102:

Q. [The Board:] I thought that [CUPP's counsel] point though was that, in his interpretation of the '344 patent or at least the embodiments that he's relying on, that disabling would actually be done by [the mobile device, not the server] . . . Can you address that?

. . .

[Trend Micro's counsel:] It's true. The mobile device would execute the command, for example the mobile device would say, okay, I'm going to block port 80 or I'm going to disable internet sharing as commanded.

. . .

Q. [The Board:] Well, isn't the argument though that the processing for that is done by the mobile device and not by the server?

A. [Trend Micro's counsel:] That was one argument, yes. So the processing is actually blocking port 80 meaning that processing happens on the mobile device.

Appx517-518 at 46:13-47:8 (emphasis added). The same is true for Trend Micro's second example, *i.e.* configuring an infrastructure entity to enforce a security policy:

It [server 102] is providing services to the mobile device. ***Sure, the server may not implement a firewall itself.*** It provides lots of other services.

Appx517 at 46:4-6 (emphasis added). Trend Micro further conceded that “infrastructure entities [] enforce security policies,” showing that the firewall security service is implemented at the infrastructure entities as a result of the infrastructure entities *processing* the security profile. Appx518 at 47:23-24. Trend Micro’s own concession undercuts any notion that server 102 actually processes Groenendaal’s profiles to implement the security service, *i.e.* enforcement of the firewall policy. Trend Micro’s admissions are further confirmation that the Board erred in failing to consider CUPP’s rebuttal evidence distinguishing Groenendaal.

Because the Board explicitly disregarded evidence and arguments rebutting Dr. Jakobsson’s bare assertion that Groenendaal implements security services by processing security code, data, and policies, it did not give CUPP “an opportunity to be heard” on this material point that defeats obviousness. Accordingly, this Court should reverse the Board’s FWD for violating the APA and fundamental requirements of due process.

### **III. THE COURT SHOULD REVERSE THE BOARD’S CONCLUSION THAT CLAIMS 8 AND 17 ARE OBVIOUS**

The Board also violated the APA and CUPP’s due process rights by determining that Claims 8 and 17 do not impose an order of operations because that decision was based on an interpretation of the “configured to mirror” term raised for

the first time at the Oral Hearing. Appx39 (quoting Appx493 at 22:20-23). The Board's construction also contradicts the plain language of the claims and logic because the relevant policies must be located on the gateway for the security system to be able to mirror them. This claim interpretation issue is dispositive because there is no dispute that the policies on Groenendaal's server 102 are not "configured to mirror" the policies on a gateway because until relevant policies are sent to Groenendaal's gateway, there are no policies that the server could possibly be configured mirror.

**A. The Board's Reliance on New Arguments at Oral Argument Violated the APA and CUPP's Due Process Rights**

As a threshold matter, the Board denied CUPP its procedural rights by relying on an argument introduced for the first time at the Oral Hearing. *See Dell Inc. v. Accelaron, LLC*, 818 F.3d 1293, 1301 (Fed. Cir. 2016) (vacating and remanding where the Board denied the patent owner its procedural rights by relying on a factual assertion introduced only during the oral argument); *see also Qualcomm Inc. v. Intel Corp.*, 6 F.4th 1256, 1264-65, 1267 (Fed. Cir. 2021) (vacating and remanding where "[t]he [oral] hearing did not provide an adequate opportunity to respond" to the Board's construction).

Specifically, in finding that the claims "do not impose an order of operations," the Board relied exclusively on Trend Micro's new argument introduced at the Oral Hearing:

Groenendaal discloses that policies are pushed from the Groenendaal server to the Groenendaal gateway. Patent Owner argues that disclosure doesn't satisfy this limitation because the policies have to be on the gateway first and are copied to the server, not vice versa. But *the claim language doesn't require an order of operations. The claim language includes the state of being mirrored.*

Appx39 (quoting Appx493 at 22:19-24) (emphasis added). Before the Oral Hearing, Trend Micro did not propose any construction for the “configured to mirror” term, let alone one that would encompass “the state of being mirrored.” *See generally* Appx129-130; Appx350-351. Nor had Trend Micro argued that the “claim language doesn't require an order of operations.” *Id.*; Appx493 at 22:20-23. CUPP was, therefore, denied any meaningful opportunity to submit arguments and evidence showing that the claims impose such an order and that Groenendaal does just the opposite. As described below, reversal is also required because this claim construction issue is dispositive.

**B. The Board Failed to Consider the Order of Operations that the Claims Require**

The Board once again collapsed the claim interpretation step into the obviousness step by looking to Groenendaal to conclude that the claims do not impose an order and include a “state of being mirrored,” *i.e.* matching policies. Appx39 (quoting Appx493 at 22:19-24). Without evaluating the intrinsic record, the Board decided that there is no order of operations and rewrote the claims to encompass that of simply matching policies, thus ensnaring Groenendaal. However,

claims are construed as written and in light of the intrinsic record. *Chef Am., Inc. v. Lamb Weston, Inc.*, 358 F.3d 1371, 1374 (Fed. Cir. 2004) (“[W]e construe the claim as written”); *Banyan Licensing, L.C. v. Orthosupport Intern., Inc.*, 34 F. App’x 696, 697 (Fed. Cir. 2002) (“First we look to the claim language” and then “we look to the rest of the intrinsic evidence”) (citations omitted).

Under a proper analysis, the claims require an order of operations because the plain claim language, logic, and the specification require an order. *Mformation Techs., Inc. v. Research in Motion Ltd.*, 764 F.3d 1392, 1399 (Fed. Cir. 2014) (“A claim requires an ordering of steps when the claim language, as a matter of logic or grammar, requires that the steps be performed in the order written, or the specification directly or implicitly requires an order of steps.”) (internal quotation marks and citations omitted). The ordering of elements applies to system claims just as it does to method claims. *Function Media, L.L.C. v. Google, Inc.*, 708 F.3d 1310, 1320-21 (Fed. Cir. 2013) (applying an order to the “creating” and “processing” elements of the system claim based, in part, on the specification). Dependent Claims 8 and 17 recite:

wherein the security code, the security policy, and the security data are configured to mirror security policies of a gateway on the trusted enterprise network

Appx71-72 (Claims 8 and 17). Accordingly, as a matter of logic, the security information on the security system can only be “configured to mirror” policies on

the gateway if those policies already exist on the gateway. Without security policies first stored on the gateway, there are no policies that the security system could be configured to mirror. Accordingly, the Board's finding that "they are both configured to mirror each other" does not make sense when there must be existing policies that the security information on the security system is configured to mirror.

The specification explains that the security policies must be located on the gateway before being translated into security policies for the security system; otherwise, there would be nothing to translate into the mobile security policy:

Further, the security administrator 325 and mobile security systems 345 can interact to automatically translate enterprise security policies into mobile security policies ***and configure mobile security systems 345 accordingly.***

Appx66 at 5:52-55 (emphasis added); *see also* Appx65 at 3:29-31 ("automatic generation of policies and data based on the policies and data on the enterprise network security system"). Accordingly, the specification requires that the security policies first be on the gateway of the enterprise network for the purpose of configuring the security information on the security system, *i.e.* configured to mirror the security policies of the gateway.

This requirement directly tracks the purpose of the claimed invention. As described in detail above, the purpose of the claimed invention is to retain the first line of defense when a mobile device travels outside the trusted enterprise network. *See supra* Statement of the Case and Facts, §§ I.A- I.B. This is achieved by claiming

a security system that is configured with the same security policies as the enterprise network. *See supra* Statement of the Case and Facts, § I.B. In this way, the security system implements the same security measures as the network security system implements on behalf of devices within the trusted enterprise network. *Id.* To carry out the purpose of the claimed invention, the security policies must be located on the enterprise network’s gateway before the security system’s policies can be configured to mirror them. Appx66 at 5:52-55.

There is no dispute that Groenendaal’s system does just the opposite. As Trend Micro concedes, Groenendaal’s architecture requires storing security and configuration profiles on server 102 and pushing those profiles to the gateway. *See, e.g.,* Appx129-130, Appx350. Because the Board’s obviousness finding is contrary to “the one permissible factual finding” that could be drawn from Groenendaal, reversal is warranted. *See Owens Corning v. Fast Felt Corp.*, 873 F.3d 896, 903 (Fed. Cir. 2017) (reversing the Board’s obviousness determination that was contrary to the “one permissible factual finding” that could be drawn from the record).

### **CONCLUSION**

CUPP respectfully requests that the Court reverse the Board’s FWD and find patentable Claims 8, 17, 19, and 20 of the ’344 Patent.

Respectfully submitted,

Dated: March 20, 2023

By: /s/ James Hannah

Paul J. Andre

James Hannah

Kramer Levin Naftalis

& Frankel LLP

333 Twin Dolphin Drive, Suite 700

Redwood Shores, CA 94065

Tel: 650.752.1700

Fax: 650.752.1810

pandre@kramerlevin.com

jhannah@kramerlevin.com

Jeffrey H. Price

Kramer Levin Naftalis

& Frankel LLP

1177 Avenue of the Americas

New York, NY 10036

Tel: 212.715.7502

Fax: 212.715.8302

jprice@kramerlevin.com

*Attorneys for Appellant*

CUPP Computing AS

**ADDENDUM**

***CUPP Computing AS v. Trend Micro Inc.***

**Appeal No. 23-1129 – IPR2021-00813**

<b>Date</b>	<b>Title</b>	<b>Appx No.</b>
10/14/2022	Final Written Decision	Appx1
	U.S. Patent No. 10,621,344	Appx50

Trials@uspto.gov  
571.272.7822

Paper 26  
Entered: October 14, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

TREND MICRO INC.,  
Petitioner,

v.

CUPP COMPUTING AS,  
Patent Owner.

---

IPR2021-00813  
Patent 10,621,344 B2

---

Before THOMAS L. GIANNETTI, GARTH D. BAER, and  
SHARON FENICK, *Administrative Patent Judges*.

GIANNETTI, *Administrative Patent Judge*.

JUDGMENT  
Final Written Decision  
Determining All Challenged Claims Unpatentable  
35 U.S.C. § 318(a)

IPR2021-00813  
Patent 10,621,344 B2

## I. INTRODUCTION

### *A. Background*

Trend Micro Inc. (“Petitioner”) filed a Petition requesting *inter partes* review of claims 1–20 (the “challenged claims”) of U.S. Patent No. 10,621,344 B2 (Ex. 1001, the “’344 patent”). Paper 1 (“Pet.”). CUPP Computing AS (“Patent Owner”) filed a Preliminary Response. Paper 6. Pursuant to 35 U.S.C. § 314, we instituted this *inter partes* review as to all of the challenged claims and all grounds raised in the Petition. Paper 7 (“Institution Dec.”).

Following institution, Patent Owner filed a Response. Paper 12 (“PO Resp.”). Subsequently, Petitioner filed a Reply to Patent Owner’s Response (Paper 15, “Pet. Reply”), and Patent Owner filed a Sur-reply (Paper 16, “PO Sur-reply”).

On July 27, 2022, we held an oral hearing. A transcript of the hearing is included in the record. Paper 25 (“Hearing Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This decision is a Final Written Decision, issued pursuant to 35 U.S.C. § 318(a). For the reasons we discuss below, we determine that Petitioner has proven by a preponderance of the evidence that all challenged claims of the ’344 patent are unpatentable.

### *B. Related Proceedings*

The parties identify the following district court proceeding concerning the ’344 patent: *CUPP Cybersecurity LLC v. Trend Micro, Inc., et al.*, No. 3:20-cv-03206 (N.D. Tex.). Pet. 1; Paper 4.

IPR2021-00813  
Patent 10,621,344 B2

A related patent, U.S. Patent No. 9,781,164 (the “’164 patent”),<sup>1</sup> was before the Board in IPR2019-00368 (the “’368 IPR”). A Final Written Decision in the ’368 IPR, finding all challenged claims of the ’164 patent unpatentable, was entered on May 28, 2020. Ex. 1005. Patent Owner’s request for rehearing by the Director of the USPTO was denied. ’368 IPR, Paper 30. The decision denying rehearing and the Board’s Final Written Decision were appealed to the Federal Circuit. ’368 IPR, Paper 31. On October 6, 2022, the Federal Circuit affirmed the Board’s Final Written Decision in the ’368 IPR. Ex. 3001.

*C. Real Party-in-Interest*

The Petition identifies Trend Micro as the real party-in-interest. Pet. 1. Patent Owner identifies CUPP Computing AS the real party-in-interest. Paper 4, 1.

*D. The ’344 Patent*

The ’344 patent describes a system and method for providing network security to mobile devices. Ex. 1001, 1:43–45. According to the patent, mobile devices are more vulnerable to attacks by malicious code when traveling outside an enterprise network. *Id.* at 2:6–10. The patent thus describes “a small piece of hardware [a ‘mobile security system’] that connects to a mobile device and filters out attacks and malicious code.” *Id.* at 2:56–60. The patent explains that “[u]sing the mobile security system, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.” *Id.* at 2:60–63.

---

<sup>1</sup> The ’344 patent is a continuation (through a chain of continuations) of the ’164 patent, and shares a common specification with the ’164 patent.

IPR2021-00813  
 Patent 10,621,344 B2

This system is illustrated in Figure 3 of the '344 patent, which follows:

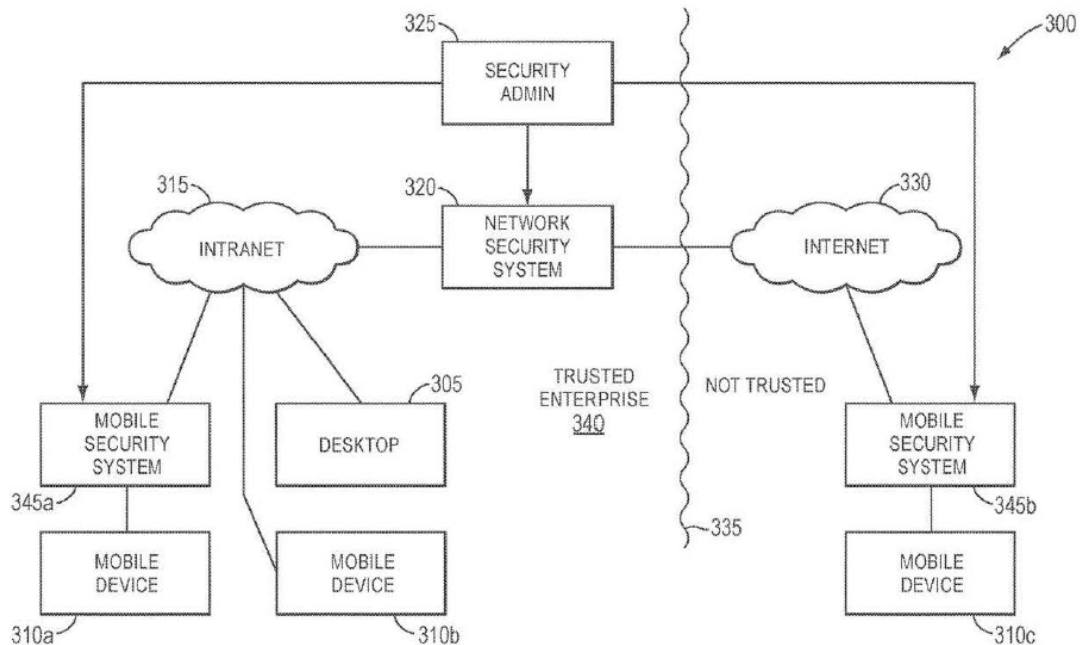


FIG. 3

Figure 3 of the '344 patent is a block diagram of a network system.

Ex. 1001, 4:12–13. Network system 300 includes desktop 305, first mobile device 310a, and second mobile device 310b. *Id.* at 4:57–60. First mobile device 310a is within trusted enterprise network 340 and is coupled to the enterprise's intranet 315 via mobile security system 345a. *Id.* at 4:60–63.

Figure 3 further shows mobile device 310c that has travelled outside trusted enterprise network 340 and is coupled to untrusted internet 330 via mobile security system 345b. *Id.* at 5:27–30. This mobile device may be in use by an employee of trusted enterprise network 340 who is currently on travel.

*Id.* at 5:10–11. Security administrator 325 manages mobile security systems 345a and 345b and network security system 320 to assure that they include the most current security protection. *Id.* at 5:11–15.

IPR2021-00813  
 Patent 10,621,344 B2

The mobile security system includes “security engines,” “security policies,” and “security data.” *Id.* at Fig. 5, 7:33–40. The administrator can update the security policies, data, and engines implemented on the mobile security system. *Id.* at 5:46–50, 11:20–25. Security administrator 325 can centrally manage all enterprise devices, remotely or directly. *Id.* at 5:50–51. Further, security administrator 325 and mobile security systems 345 can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security systems 345. *Id.* at 5:52–55.

### *E. Illustrative Claims*

The ’344 patent has twenty claims, all of which are challenged in the Petition. Claims 1, 10, 19, and 20 are independent. Claims 1 and 19 are representative of the claims. Claim 1 recites<sup>2</sup>:

1. A security system, comprising:

[1.1] security system memory; and

[1.2] a security system processor configured to:

[1.3] store in the security system memory at least a portion of security code, at least a portion of a security policy, and at least a portion of security data,

[1.4] the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to provide security services to a mobile device coupled to the security system, the mobile device having at least one mobile device processor different than the security system processor of the security system,

[1.5.] the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being managed by one or more information

---

<sup>2</sup> Paragraph numbering provided by Petitioner has been added.

IPR2021-00813

Patent 10,621,344 B2

technology (IT) administrators using an IT administrator system on a trusted enterprise network, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network, the mobile device being a first computer system, the security system being a second computer system, and the IT administrator system being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems;

[1.6] store in the security system memory at least a portion of remote management code configured to process an update command, the update command being an instruction to update at least one of the security code, the security policy, or the security data based on one or more revised policies implemented by the one or more IT administrators on the trusted enterprise network;

[1.7] receive a particular update command to update a particular one of the security code, the security policy, or the security data, the particular update command having originated from the IT administrator system and having been forwarded to the security system; and

[1.8] execute the update command using the remote management code to update the particular one of the security code, the security policy, or the security data.

Ex. 1001, 15:20–67.

Claim 19 recites:

19. A security system, comprising:

[19.1] security system memory; and

[19.2] a security system processor configured to:

[19.3] store in the security system memory at least a portion of security code, at least a portion of a security policy, and at least a portion of security data,

IPR2021-00813

Patent 10,621,344 B2

[19.4] the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to be processed by the security system processor to implement security services for a mobile device coupled to the security system, the mobile device having at least one mobile device processor different than the security system processor of the security system,

[19.5] the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being managed by one or more information technology (IT) administrators using an IT administrator system on a trusted enterprise network, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network, the mobile device being a first computer system, the security system being a second computer system, and the IT administrator system being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems;

[19.6] store in the security system memory at least a portion of remote management code configured to process an update command, the update command being an instruction to update at least one of the security code, the security policy, or the security data based on one or more revised policies implemented by the one or more IT administrators on the trusted enterprise network;

[19.7] receive a particular update command to update a particular one of the security code, the security policy, or the security data, the particular update command having originated from the IT administrator system and having been forwarded to the security system; and

[19.8] execute the update command using the remote management code to update the particular one of the security code, the security policy, or the security data.

Ex. 1001, 17:41–18:24.

IPR2021-00813  
Patent 10,621,344 B2

Claims 10 and 20 are directed to computer-readable storage devices and are similar to claims 1 and 19, respectively.

*F. References and Other Evidence*

Petitioner relies on the following reference: U.S. Patent App. Pub. No. 2005/0260996 (Ex. 1003, “Groenendaal”).

Petitioner relies also on a Declaration of Dr. Markus Jakobsson (Ex. 1019, “Jakobsson Decl.”). Patent Owner relies on a Declaration of Michael T. Goodrich, Ph.D. (Ex. 2002, “Goodrich Decl.”). The parties have submitted deposition transcripts for those witnesses. Ex. 1020 (“Goodrich Dep.”); Ex. 2004 (“Jakobsson Dep.”). In addition, the parties have submitted several expert declarations and deposition transcripts from the ’368 IPR.<sup>3</sup>

*G. Asserted Ground of Unpatentability*

Petitioner asserts the challenged claims are unpatentable on the following ground (Pet. 3):

<b>Claims Challenged</b>	<b>Basis (35 U.S.C.)<sup>4</sup></b>	<b>Reference</b>
1–20	§ 103(a)	Groenendaal

<sup>3</sup> Patent Owner has submitted Dr. Jakobsson’s initial and supplemental declarations and deposition transcript from the ’368 IPR. Exs. 2003, 2005, 2006. In addition, the parties have submitted a declaration (Ex. 2007) and deposition transcript (Ex. 1011) of Nenad Medvidovic, Ph.D., from the ’368 IPR. Dr. Medvidovic testified for Patent Owner in the ’368 IPR.

<sup>4</sup> Because the earliest application from which the ’344 patent issued was filed before March 16, 2013, the pre-AIA (“America Invents Act”) version of §103 applies. Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 285–88 (2011).

IPR2021-00813  
Patent 10,621,344 B2

## II. PRELIMINARY MATTERS

### *A. Level of Ordinary Skill*

Petitioner contends “[a] person of ordinary skill in the art at the time of the alleged invention of the ’344 patent (i.e., December 13, 2005) . . . would have had a Bachelors’ degree in computer science, electrical engineering, or a comparable field of study, plus at least two years of professional experience with computer security systems, or the equivalent.” Pet. 6 (citing Jakobsson Decl. ¶¶ 52–53).

Patent Owner does not provide a formulation of the person of ordinary skill. Dr. Goodrich, however, provides the following testimony: “In my opinion, a person of ordinary skill in the art in the field of the ’344 Patent as of its priority date would be someone with a bachelor’s degree in computer science or related field, and either (1) two or more years of industry experience and/or (2) an advanced degree in computer science or related field.” Goodrich Decl. ¶ 31. The two formulations differ only slightly. For example, Dr. Jakobsson is more specific in requiring “professional experience with computer security systems, or the equivalent.” Jakobsson Decl. ¶ 52.

Petitioner’s definition is supported by credible expert testimony and is more consistent with the prior art and the patent specification before us. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (prior art itself may reflect an appropriate level of skill). We, therefore, adopt Petitioner’s description, but without the qualifier “at least.”<sup>5</sup> However, we would reach

---

<sup>5</sup> Including “at least” suggests a broader and open-ended level of ordinary skill than that expressly stated by Petitioner. This change, however, does not affect the outcome of our analysis.

IPR2021-00813  
Patent 10,621,344 B2

the same result under either the formulation proposed by Petitioner or that suggested by Dr. Goodrich.

*B. Description of the Groenendaal Reference*

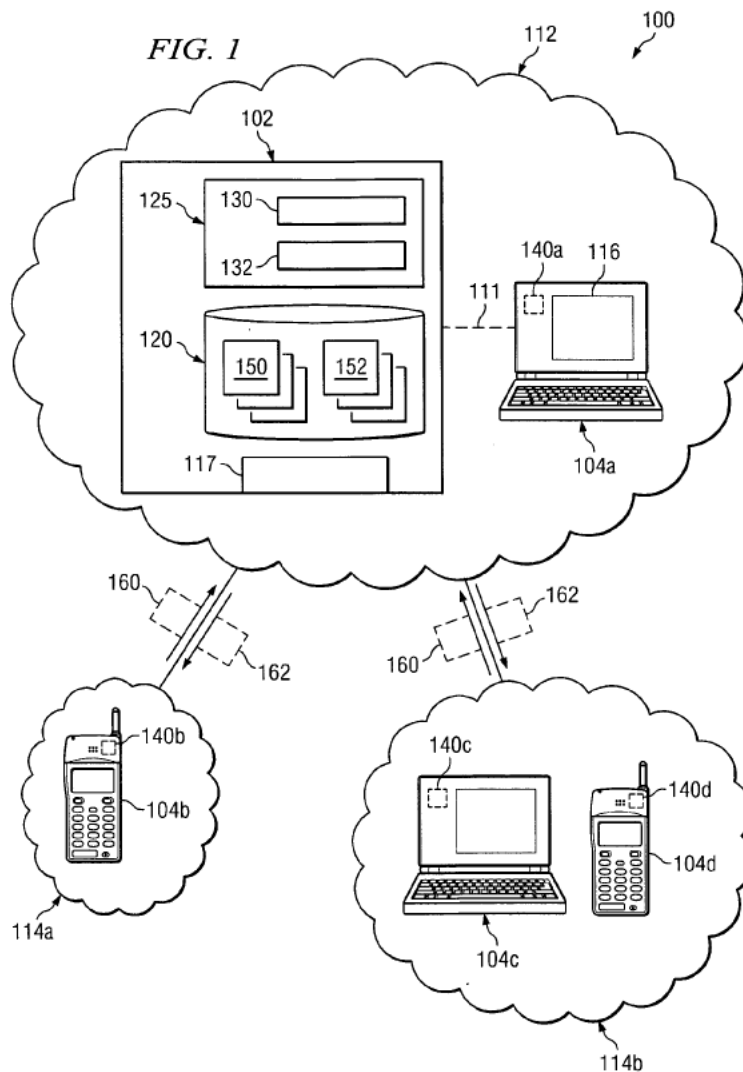
Groenendaal describes a wireless agent for a mobile device.

Ex. 1003, (57). In one embodiment, the wireless agent is operable to dynamically determine an access point for wireless communications from a mobile device through a network. *Id.* The wireless agent is further operable to automatically select one of a plurality of security profiles associated with a mobile device based, at least in part, on the determined access point. *Id.*

Each security profile includes a plurality of security parameters for accessing a wireless network. The wireless agent then modifies at least one of a plurality of network configuration options of the mobile device based on the selected security profile, and automatically attempts to connect the mobile device to the access point using the network configuration options. *Id.*

IPR2021-00813  
 Patent 10,621,344 B2

Petitioner relies on Figure 1 of Groenendaal, which follows:



Pet. 17. Figure 1 of Groenendaal shows security management system 100 including server 102 and enterprise network 112. Ex. 1003 ¶ 16. The server includes security manager 130 and configuration manager 132. *Id.* ¶ 20. The server also includes memory 120 that stores security profiles 150 and configuration profiles 152. *Id.* ¶ 17.

The security system provides security services to mobile clients 104 (e.g., 104b, 104c, and 104d). *Id.* ¶ 14. For example, an administrator manages and updates the security profiles and configuration profiles using

IPR2021-00813  
 Patent 10,621,344 B2

GUI (graphical user interface) 116 on laptop 104a. *Id.* ¶¶ 27, 28. The configurable and updatable security policies relate to firewall settings, intrusion detection, file sharing, network authentication, and allowed and disallowed network access points, among other security services. *Id.* ¶¶ 57–60, Figs. 4–6.

### *C. Claim Construction*

In an *inter partes* review, the claims of a patent shall be construed using the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b), including construing the claims in accordance with the ordinary and customary meaning of such claims as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005). Under that standard, and absent any special definitions, we give claim terms their ordinary and customary meaning, as would be understood by one of ordinary skill in the art at the time of the invention. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

Any special definitions for claim terms must be set forth with reasonable clarity, deliberateness, and precision. *See In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Extrinsic evidence is “less significant than the

IPR2021-00813  
 Patent 10,621,344 B2

intrinsic record in determining the legally operative meaning of claim language.” *Phillips*, 415 F.3d at 1317 (internal quotes and citation omitted).

We construe claim terms only as relevant to the parties’ contentions and only to the extent necessary to resolve the issues in dispute. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999); *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

Both Petitioner and Patent Owner address claim construction and ask us to construe terms in the challenged claims. Pet. 6–15; PO Resp. 12–16.

*1. “provide security services to a mobile device” (Claims 1, 10)*

Independent claims 1 and 10 call for “a portion of the security data configured to provide security services to a mobile device coupled to the security system.” In our ’368 IPR Institution Decision, we determined that this phrase should be construed to encompass the distribution of security information to a mobile device, without more. Ex. 1004, 8–9.<sup>6</sup> In our Final Written Decision in the ’368 IPR, after reviewing the evidence presented during the trial, we maintained that construction. Ex. 1005, 11–12.

Petitioner asks us to adopt the same construction in this proceeding. Pet. 6. Petitioner points out that “[p]roviding updated security information to the mobile device is a security service because doing so can, for example, protect the mobile device against newly identified threats, or configure it for securely connecting to new networks.” *Id.* (citing Jakobsson Decl. ¶ 57; Ex. 1001, 2:34–37). Petitioner relies also on dictionary definitions from *Merriam-Webster’s Collegiate Dictionary* (11th ed., 2007), defining

---

<sup>6</sup> Unless otherwise specified, citations to exhibits use the page numbers assigned by the parties and not the original page numbers.

IPR2021-00813

Patent 10,621,344 B2

“service” as including “the occupation or function of serving,” “the work performed by one that serves,” and “HELP, USE, BENEFIT” (Ex. 1008, 3); *The Microsoft Internet & Networking Dictionary* (2003), defining “service” as including “a program or routine that provides support to other programs” (Ex. 1009, 3); and *Webster’s Collegiate Dictionary* (2002), defining “service” as “[t]he act or occupation of serving,” which would include serving information (Ex. 1010, 3). Pet. 7.

The term “security services” does not appear in the written description of the ’344 patent. However, in the Figure 3 embodiment, described *supra*, the mobile security device is described as effectively “a mobile internet gateway on behalf of the mobile device 310c.” Ex. 1001, 5:32–34. Furthermore, the specification of the ’344 patent describes how the security administrator manages the mobile device by providing updates to the mobile security system. *See, e.g.*, the following description of the Figure 3 embodiment from the ’344 patent:

In this embodiment, because the security administrator 325 is capable of remotely communicating with the mobile security system 345b, *IT can monitor and/or update the security policies/data/engines implemented on the mobile security system 345b.* The security administrator 325 can centrally manage all enterprise devices, remotely or directly. *Further, the security administrator 325 and mobile security systems 345 can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security systems 345 accordingly.* Because the mobile security system 345 may be generated from the relevant security policies of the enterprise 340, the mobile device 310c currently traveling may have the same level of protection as the devices 305/310 within the trusted enterprise 340.

Ex. 1001, 5:46–60 (emphasis added). In this example from the specification, the security administrator provides security services to a mobile device by

IPR2021-00813

Patent 10,621,344 B2

monitoring and updating the security policies implemented on the mobile security system and by interacting with the mobile security system to automatically translate enterprise security policies into mobile security policies and configuring mobile security systems accordingly. The '344 patent explains also that the security administrator and the security system “can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security systems . . . accordingly.” *Id.* at 5:52–55. Therefore, we agree with Petitioner and find that the proper construction of “provide security services to a mobile device” in claims 1 and 10 includes sending security information to the mobile device, as it is consistent with the description in the specification of the security administrator managing the security of the mobile devices.

Patent Owner does not address directly this proposed construction. *See generally* PO Resp. 12–26. However, in discussing Groenendaal, Patent Owner implicitly challenges this construction by making the argument that “*Groenendaal* teaches the well-known prior art technique of transferring security policies to a mobile device without any separate security system processing security information and implementing security services on its behalf.” *Id.* at 12; *see also id.* at 28 (“*Groenendaal* is directed to pushing security profiles from a server to a mobile device, where the mobile device itself implements any attendant security services.”).

We disagree with this argument by Patent Owner implicitly limiting the scope of “provid[ing] security services,” and, for the reasons given by Petitioner, we find that “[p]roviding updated security information to the mobile device is a security service because doing so can, for example, protect the mobile device against newly identified threats, or configure it for

IPR2021-00813

Patent 10,621,344 B2

securely connecting to new networks.” Pet. 6 (citing Jakobsson Decl. ¶ 57; Ex. 1001, 2:34–37).

2. “*implement security services for a mobile device*” (claims 19 and 20)

Consistent with its position on the “security services” recitation in claims 1 and 10, Petitioner contends the plain meaning of this limitation appearing in independent claims 19 and 20 “includes sending security information to a mobile device.” Pet. 8. Petitioner supports this construction with testimony from Dr. Jakobsson (Jakobsson Decl. ¶¶ 62–64) and a dictionary definition of “implement” as “CARRY OUT, ACCOMPLISH.” Pet. 8 (quoting Ex. 1012, 3). Based on this definition of “implement” from *Merriam-Webster’s Collegiate Dictionary*, (11<sup>th</sup> ed.), Petitioner contends “carrying out or accomplishing the act of providing security information to a mobile device is implementing that security service.” *Id.*

Patent Owner addresses this limitation in connection with its alternative construction of the “configured to be processed” limitation, discussed *infra* in Section II.C.4. For the reasons given by Petitioner and in our discussion, *infra*, of “configured to be processed,” we find that the proper construction for “implement security services for a mobile device” is “carrying out or accomplishing an action, such as providing security information to a mobile device.” Pet. 8; Jakobsson Decl. ¶¶ 62–64.

Patent Owner contends that the term “implement” means “put into effect.” PO Resp. 20. Despite Patent Owner’s treatment of this claim construction issue as dispositive, however, we agree with Petitioner that Groenendaal discloses this limitation even under Patent Owner’s construction, by providing (i.e., “putting into effect”) security services

IPR2021-00813  
Patent 10,621,344 B2

beyond providing security profiles to the mobile device. *See* Pet. 24–27; Pet. Reply 17–21. This is further discussed *infra*, in Section III.B.5.

3. “*configured based on one or more policies implemented by the one or more IT administrators*” (claims 1, 10, 19, 20)

These independent claims recite “one or more policies implemented by the one or more IT administrators on the trusted enterprise network.” *See, e.g.*, claim elements 1.5, 19.5, *supra*. Petitioner contends that the “one or more policies” recited in these claims differ from the separately-recited stored “security policy” in claim limitations 1.3 and 19.3. Pet. 8–11. Petitioner contends that “the plain and ordinary meaning of ‘one or more policies’ does not require these policies be stored in computer memory.” *Id.* at 8–9. Petitioner explains that “the ‘one or more policies’ can include decisions made by the recited ‘one or more IT administrators.’” *Id.* at 9. Petitioner provides the following example: “[A] company may have a policy that employees may not access social media, which is different than the stored implementation in the form of a list of prohibited URLs.” *Id.* As Petitioner points out, this construction is consistent with our findings in the ’368 IPR. *Id.* at 9 (citing Ex. 1005, 32).

Patent Owner contends that the term “configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network” should be accorded its “plain and ordinary meaning.” PO Resp. 20. Patent Owner asserts that the “one or more policies” do not encompass policies in the mind of the IT administrator. *Id.* at 21. As discussed *supra*, according to Patent Owner, the term “implemented” means “put into effect.” *Id.* at 20. Thus, Patent Owner asserts the claimed “security policy, security code, and security data” must

IPR2021-00813  
Patent 10,621,344 B2

be “configured based on one or more policies *put into effect* by one or more IT administrators operating on the trusted enterprise network.” *Id.* (emphasis added). According to Patent Owner, this would exclude “the mental decisions of an IT administrator.” *Id.* at 21–25.

We do not agree with this limiting construction by Patent Owner. As we concluded in the ’368 IPR Final Written Decision, we find that the claims do not require that the security data be based on policies “put into effect.” Ex. 1005, 14–15. As we observed in the ’368 IPR, the claims require that the policies be “implemented.” *Id.* at 14. We construe this *supra* as “carrying out or accomplishing an action.” The claims themselves identify separately (1) the security code, security policy, and security data “being managed” by the IT administrators, and (2) the “policies implemented” by the IP administrators. *Compare* Ex. 1001, 15:33–38 with 15:41–43. The ’344 patent specification, likewise, distinguishes between the security code, security policy, and security data and the policies implemented by the administrators. Thus, the specification describes an embodiment where the security code, security policy, and security data are “based on” IT decisions or user preferences:

In an embodiment where the mobile security system 345 supports multiple mobile devices 310, the security engines 530, security policies 535 and security data 540 may be different for each mobile device 310 (*e.g., based on for example user preferences or IT decision*).

Ex. 1001, 10:41–45 (emphasis added).

For the reasons given by Petitioner and those summarized above, we adopt a construction of this limitation that includes “one or more policies” that are not necessarily “in computer memory.” Pet. 8–10. We find, as Petitioner contends, that “[t]he configuration of this limitation need be based

IPR2021-00813  
Patent 10,621,344 B2

only on the policies; it does not also need to be based on the implementation of those policies.” *Id.* at 12.

We rely on the “plain meaning” of the claim language. As Petitioner explains, “in the claim language ‘configured based on one or more policies implemented by the one or more IT administrators,’ the clause ‘implemented by the one or more IT administrators’ simply indicates which policies may serve as the basis for the configuration.” *Id.* at 13.

We rely also on the ’344 patent specification, specifically, the above embodiment where the configuration of the security code, security policy, and security data are “based on” an IT decision. *Id.* at 13–14 (citing Ex. 1001, 10:41–47, 14:65). We reject Patent Owner’s belated attempt at the hearing to marginalize this disclosure as an “unclaimed embodiment.” Hearing Tr. 30:12–13. We have seen nothing in the intrinsic record that would support a disavowal of this embodiment by Patent Owner. “To disavow claim scope, the specification must contain ‘expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope.’” *Retractable Techs., Inc. v. Becton, Dickinson & Co.*, 653 F.3d 1296, 1306 (Fed. Cir. 2011) (quoting *Epistar Corp. v. Int’l Trade Comm’n*, 566 F.3d 1321, 1335 (Fed. Cir. 2009)).

For the reasons given, we find that this limitation includes configurations that are not necessarily based on the implementations of policies, but are based on IT administrator decisions. Pet. 11–12. This is consistent with our findings in the ’368 IPR Final Written Decision. *See* Ex. 1005, 15.

As we also observed in that Final Written Decision, and for reasons discussed *infra*, this construction issue is not dispositive, as the Groenendaal

IPR2021-00813

Patent 10,621,344 B2

reference discloses this limitation, even under Patent Owner’s contentions regarding this limitation. *See* discussion *infra*, in Section III.B.6.

4. “*the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to be processed by the security system processor to implement security services for a mobile device coupled to the security system*” (Claims 19 and 20)

Patent Owner proposes that the phrase “processed by the security system processor to implement security services for a mobile device,” from claim limitation 19.4 (but not present in claim element 1.4), be “accorded its plain and ordinary meaning.” PO Resp. 13. Drawing a distinction to claim element 1.4, Patent Owner continues, “[t]he plain language of claims 19 and 20 expressly requires security services be ‘implement[ed] . . . for’ a mobile device, rather than merely ‘provide security services to a mobile device’.” *Id.* at 14 (emphasis omitted; alterations in original).

Patent Owner argues that the Board should reject Petitioner’s construction of “implement security services for a mobile device” in claim 19 because it is “unsupported by the intrinsic record.” *Id.* at 16–18. Patent Owner repeats its argument that “[c]ontrary to Petitioner’s proposal, the plain and ordinary meaning of the term ‘configured to be processed by the security system processor to implement security services for a mobile device coupled to the security system’ does not encompass the mere distribution or sending of security information to a mobile device, without more.” *Id.* at 16.

Petitioner contends that the language added to claim 19, like claim limitation 1.4, “includes providing security services to a mobile device.” Pet. 26. But Petitioner contends that even under Patent Owner’s

IPR2021-00813  
Patent 10,621,344 B2

construction, Groenendaal provides “additional security services” that involve processing by the server to implement security services for mobile devices. *Id.*; Pet. Reply 17–21. Petitioner argues that “[t]hese security services satisfy this limitation even under Patent Owner’s interpretation of this limitation because they go beyond merely providing security information to a mobile device.” Pet. Reply 17–18. One example is the description of Groenendaal’s server configuring a firewall policy for a given user on a wireless gateway when the user enters a particular access-zone. *Id.* at 19 (citing Ex. 1003 ¶ 14). Petitioner explains that in this example, “[t]he server’s doing so implements a security service because it accomplishes a security-related task that is helpful to the mobile device.” *Id.*

Patent Owner responds to this argument by imposing an additional, restriction on the term “implement.” PO Sur-reply 17–20. Patent Owner asserts, specifically referring to the firewall policy, that “this profile information is enforced onto an agent or by configuring another infrastructure entity, e.g., access point or gateway, to enforce security policies.” *Id.* at 20. Thus, Patent Owner argues,” [i]n Groenendaal, the server is never implementing security services for any other device. At best, it tells other devices what to do and the device does it itself.” Hearing Tr. 32:11–13.

We reject this implicit restriction, which would amount to a rewriting of the claim. Patent Owner’s restriction would require the security system processor *alone* to provide services to the mobile device, without the involvement of “another infrastructure entity” such as a gateway. *Id.*; *see also id.* at 34:18–19 (characterizing Groenendaal’s server 102 as “merely a conduit”), 56:10–56:24. Nothing in the claim requires the security system

IPR2021-00813

Patent 10,621,344 B2

processor *by itself* to “implement” security policies, without sending security information to an “infrastructure entity” such as a gateway to provide a service (such as a firewall) to the mobile device. Excluding such a firewall arrangement is inconsistent with Patent Owner’s description of the ’344 patent as providing “an additional line of defense for the mobile device.” PO Resp. 8.

Furthermore, as will be discussed in greater detail in connection with our analysis of Groenendaal, *infra*, the processing of security information by a security system and implementing security services by providing security information to a mobile device (or to an entity such as a gateway for the benefit of the mobile device), are not mutually exclusive activities, as implied by Patent Owner’s proposed construction. Dr. Jakobsson testifies that Groenendaal discloses several examples of implementing security services for a mobile device that also involve the security server processing security information:

Groenendaal also discloses implementing security services for a mobile device beyond providing security information to the mobile device, as established for limitation 1.4 . . . . Each of these services is implemented by the security server processor by processing the stored security code, security policies, and security data, as established for limitation 1.4.

Jakobsson Decl. ¶ 105. Thus, while we agree with Petitioner’s construction, we also agree that Groenendaal meets this limitation under Patent Owner’s construction. *See infra*, Section III.B.5.

We have considered Patent Owner’s additional arguments and find them unavailing. For example, Patent Owner contrasts the recitation in claim 19 of “configured to be processed to implement security services for

IPR2021-00813  
Patent 10,621,344 B2

the mobile device” with the recitation in claim 1 of “configured to provide security services to a mobile device.” PO Resp. 5–8. Based on this difference, Patent Owner asserts “the ’344 Patent’s additional claim limitation expressly requires security services be implemented for a mobile device, rather than merely “providing security services to a mobile device.” *Id.* at 8 (emphasis omitted). At the oral argument, Petitioner’s counsel acknowledged this difference in claim scope, but argued that “both limitations read on Groenendaal.” Hearing Tr. 45:16–21. We agree that Groenendaal meets both constructions, as is discussed *infra* in Section III.B.5.

For the reasons given, therefore, we do not adopt Patent Owner’s construction, including the proposed restriction of the term “configured to be processed by the security system processor to implement security services for a mobile device” as requiring the processor *alone* to provide the security services, without the involvement of other entities.

#### 5. *Additional Terms*

To the extent necessary, we address the parties’ contentions regarding the term “configured to mirror,” found in claims 8 and 17, in Section III.D, *infra*. No other constructions are necessary to resolve the issues in dispute. *Vivid Techs., Inc.*, 200 F.3d at 803.

### III. ANALYSIS OF THE CHALLENGED CLAIMS

The Petition challenges claims 1–20 of the ’344 patent. Petitioner asserts unpatentability of the claims based on obviousness. Pet. 3.

#### A. *Obviousness*

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject

IPR2021-00813  
 Patent 10,621,344 B2

matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007).

The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) so-called “secondary considerations,” including commercial success, long-felt but unsolved needs, failure of others, and unexpected results. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966) (“the *Graham* factors”). Neither the Petition nor the Patent Owner has presented evidence on the fourth *Graham* factor. We therefore do not consider that factor in this decision.

Petitioner contends claims 1–20 would have been “obvious . . . in light of Groenendaal.” Pet. 15. As mentioned above, claims 1, 10, and 19, and 20 are independent. Petitioner combines its analysis of claim 1 with claim 19. We therefore address claim 1 and 19 together. *Id.* at 18–47.

### *B. Claims 1 and 19*

Petitioner’s “limitation-by-limitation analysis” of claims 1 and 19 in relation to Groenendaal appears at pages 18–47 of the Petition. Petitioner supports its analysis with testimony from its expert, Dr. Jakobsson. Jakobsson Decl. ¶¶ 87–149. For the reasons that follow, we find that each limitation of claims 1 and 19 is disclosed or suggested by Groenendaal.

#### *1. Preambles*

The preambles of claims 1 and 19 each recite a “security system.” Petitioner contends this element is found in Groenendaal’s server 102. Pet. 18 (citing Ex. 1003, Fig. 1, ¶¶ 16, 20). Patent Owner does not challenge

IPR2021-00813  
 Patent 10,621,344 B2

this assertion. We find, based on the evidence presented by Petitioner, that Groenendaal teaches the preambles of claims 1 and 19.<sup>7</sup>

## 2. *Elements 1.1, 19.1*

Claim 1 and 19 both call for a “security system memory.” *See* claim elements 1.1, 19.1, *supra*. Petitioner contends that this element is met by memory 120 in server 102 of Groenendaal. Pet. 18 (citing Ex. 1003, Fig. 1, ¶¶ 16–17). Patent Owner does not challenge this assertion. We find, based on the evidence presented by Petitioner, that Groenendaal teaches claim elements 1.1 and 19.1.

## 3. *Elements 1.2, 1.3, 19.2, 19.3*

Claims 1 and 19 both call for “a security system processor configured to: store in the security system memory at least a portion of security code, at least a portion of a security policy, and at least a portion of security data.” *See* claim elements 1.2, 19.2, *supra*. Petitioner contends the “security system” limitation is met by Groenendaal’s server 102 and the “processor” limitation by processor 125 included in the server. Pet. 18 (citing Ex. 1003 ¶¶ 16, 20, Fig. 1). Petitioner explains that “because processor 125 executes the wireless manager, it is configured to perform the server functionality that satisfies the remaining limitations of this claim, described below” (referring to claim elements 1.3–1.8, *supra*, and citing Jakobsson Decl. ¶ 89).

Patent Owner does not challenge Petitioner’s identification of the processor in Groenendaal with the claimed security system processor. We find, based on the evidence presented by Petitioner, that Groenendaal teaches the security system processor of claim elements 1.2 and 19.2.

---

<sup>7</sup> We do not express an opinion on whether these preambles are limiting.

IPR2021-00813  
 Patent 10,621,344 B2

Petitioner contends that the “store” limitation of claim elements 1.3 and 19.3 (“store in the security system memory . . .”) is met by Groenendaal’s disclosure of memory 120 storing security profiles 150 and configuration profiles 152. Pet. 19 (citing Ex. 1003 ¶¶ 21, 23). Petitioner explains that “[s]ecurity profile 150 includes any parameters, variables, policies, algorithms, instructions, or rules for securing clients 104, and configuration profile 152 includes any parameters, variables, policies, algorithms, instructions, settings, or rules, including security settings, for wirelessly connecting clients 104.” *Id.* (citing Ex. 1003 ¶¶ 18–19) (internal quotation marks omitted). Also, “[a]n administrator may create and update these stored profiles, including their security code, security policies, and security data, using the graphical user interface (‘GUI’) shown in Figs. 7A–E, 8A–K, 9A–B.” *Id.* (citing Ex. 1003 ¶¶ 20, 28, 58–60).

Patent Owner does not challenge the assertion that Groenendaal stores policies, although Patent Owner disputes Petitioner’s identification of the stored policies. *See* discussion of “one or more policies” in Section II.C.3, *supra*.

Petitioner contends that the stored policies in claim elements 1.3/19.3 are not the same as the “one or more policies” recited in claim elements 1.5/19.5. Pet. 8. Petitioner contends that the “one or more policies” in 1.5/19.5 do not have to be stored in computer memory. *Id.* at 8–9; Pet. Reply 6. For the reasons given by Petitioner, we agree. Pet. 18–22; Pet. Reply 8–11. As discussed in Section II.B.3, *supra*, and in our Final Written Decision in the ’368 IPR, “[c]onsistent with this claim language, we find that there is a distinction between policies implemented by the IP administrators and the ‘security code, security policy, and security data’

IPR2021-00813  
 Patent 10,621,344 B2

described in the claim as ‘stored in the memory of the computer system.’”  
 Ex. 1005, 33. We further find, based on our construction of “one or more policies” and the above reasons presented by Petitioner, that Groenendaal teaches claim elements claims 1.3 and 19.3. Jakobsson Decl. ¶¶ 90–96.

#### 4. *Element 1.4*

Claim 1 further calls for “the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to provide security services to a mobile device coupled to the security system, the mobile device having at least one mobile device processor different than the security system processor of the security system.” *See* claim element 1.4, *supra*. Petitioner contends the “different processors” limitation (“the mobile device having at least one mobile device processor different than the security system processor of the security system”) is met by Groenendaal: “Mobile devices 104 have ‘one or more processors’ different than the processor of server 102 (security system). [Ex. 1003] ¶¶ 27, 20, Fig. 1 (showing mobile devices 104 as separate from the server 102).” Pet. 22. The contention that the “different processors” limitation is met by Groenendaal is not disputed by Patent Owner. We find that Groenendaal meets this limitation for the reasons given by Petitioner. Jakobsson Decl. ¶ 97.

Petitioner further explains that Groenendaal meets the “configured to provide” limitation: “Groenendaal also discloses that the security code, security policy, and security data described above are configured to provide security services to mobile clients 104.” Pet. 22. Petitioner gives examples, such as Groenendaal’s description of security profiles 150 as including “‘any parameters, variables, policies, algorithms, instructions, or rules for securing

IPR2021-00813  
Patent 10,621,344 B2

clients 104,’ (a security service).” *Id.* (citing Ex. 1003 ¶ 18); *see also id.* at 22–24 (further examples include an administrator “dynamically manag[ing] network security features of clients 104,” “server 102’s ‘wireless manager,’” and “distributed” security profiles 150). We find that Patent Owner’s response, that Groenendaal does not provide security services because it is directed to “pushing security profiles from a server to a mobile device,” is unavailing because it is contrary to our claim construction. *See supra*, Section II.C.1. Accordingly, we find that under our claim construction Petitioner demonstrates that Groenendaal meets this limitation. Jakobsson Decl. ¶¶ 98–100.

Anticipating Patent Owner’s argument that sending security information to a mobile device is not providing security services (*see supra*, Section II.C.1), Petitioner demonstrates also that Groenendaal also discloses that the stored security code, policy, and data provide security services to the mobile devices *other* than by sending security profiles 150. Pet. 24–26; Pet. Reply 17–22. For example, Petitioner demonstrates that Groenendaal discloses that security manager 130 may command client 104 “to perform an action such as shut down wireless access, block port, disable Internet sharing, and lose other privileges.” Pet. 24 (citing Ex. 1003 ¶ 21). Petitioner’s expert, Dr. Jakobsson, provides other examples of similar disclosures in Groenendaal. Jakobsson Decl. ¶¶ 101–103. He testifies that Groenendaal’s server may configure “infrastructure entities” to enforce the security policies. *Id.* ¶ 101 (emphasis omitted). For example, the server can configure or implement a firewall policy for a given user on a wireless gateway. *Id.* (citing Ex. 1003 ¶ 14). Petitioner contends that these “additional security services” meet this limitation even under Patent

IPR2021-00813  
Patent 10,621,344 B2

Owner’s claim construction. Pet. 24–26; Pet. Reply 17–18 (“These security services satisfy this limitation even under Patent Owner’s interpretation of this limitation because they go beyond merely providing security information to a mobile device.”).

Patent Owner responds that Groenendaal “is directed to pushing security profiles from a server to a mobile device, where the mobile device itself implements any attendant security services.” PO Resp. 28 (citing Goodrich Decl. ¶ 87). As to Dr. Jakobsson’s examples of the stored security code, policy, and data in Groenendaal providing security services to the mobile devices other than by sending security profiles, Patent Owner contends these do not meet the claim limitation because they are “implemented by the mobile device.” *Id.* at 31. Specifically, as to the firewall example, Patent Owner contends “the enabled profile is implemented on and by the mobile device, not the server.” *Id.*

We do not agree that these arguments by Patent Owner distinguish Groenendaal’s disclosures from the challenged claims. For the reasons presented *supra*, we construe “provide security services to a mobile device” as including providing security information to the mobile device. *See supra*, Section II.C.1. We find that under this construction, Groenendaal meets this claim limitation, for example, by providing updated security information to the mobile devices. Pet. 6 (citing Jakobsson Decl. ¶ 57; Ex. 1001, 2:34–37).

But even if we had adopted a more restrictive construction for this limitation that would exclude sending security information to a mobile device, we find that Petitioner’s example of configuring or implementing firewall protection for the mobile devices would meet the limitation. Pet. 24; Pet. Reply 20; Jakobsson Decl. ¶ 101. Patent Owner’s attempt to

IPR2021-00813  
 Patent 10,621,344 B2

distinguish the firewall example by arguing that Groenendaal’s firewall is not implemented on the server because a gateway is involved is unavailing. *See, e.g.*, Hearing Tr. 55:23–56:2; *see also* discussion of “additional security services” in Section II.C.4, *supra*. As discussed in that Section, we do not agree with Patent Owner’s contention that due to the presence of the gateway, the server does not provide the claimed security services to the mobile device.

We find that for the reasons given by Petitioner, summarized *supra*, these additional services, and particularly processing on the server to set up the firewall for the mobile device in Groenendaal, meet this claim limitation. Jakobsson Decl. ¶¶ 101–103. As Dr Jakobsson testifies, “[e]ach of these services is implemented by the security server processor by processing the stored security code, security policies, and security data, as established for limitation 1.4.” *Id.* ¶ 105.

We find, based on the evidence presented by Petitioner, that Groenendaal teaches claim element 1.4.

#### 5. *Element 19.4*

Claim element 19.4, similar (but not identical to) claim element 1.4, calls for “the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data *configured to be processed by the security system processor to implement security services* for a mobile device coupled to the security system.” Ex. 1001, 17:47–52 (emphasis added). As noted by Patent Owner, the language italicized above in claim element 19.4 above differs from element 1.4. PO Resp. 7. However, we declined to adopt Patent Owner’s proposed construction of the “configured to be processed” limitation in claim 19. *See*

IPR2021-00813  
 Patent 10,621,344 B2

Section II.C.4, *supra*. We observed, however, that “while we agree with Petitioner’s construction, we also agree that Groenendaal meets this limitation under Patent Owner’s construction.” *Id.*

For this claim element, Petitioner relies on its analysis of similar claim element 1.4. Pet. 26. For the reasons set forth in connection with claim element 1.4, *supra*, we find that Petitioner demonstrates that Groenendaal meets the common limitation “implement security services for a mobile device” under the construction we have adopted. *See* Section II.C.4, *infra*.

Responding to Patent Owner’s construction of this limitation, Petitioner demonstrates that even under Patent Owner’s construction, “Groenendaal discloses implementing security services for a mobile device beyond providing security information to the mobile device.” Pet. 26–27. We find that these additional security services meet the claim construction proposed by Patent Owner for the reasons given by Petitioner. *Id.*

Petitioner cites Groenendaal’s “firewall policy for a given user” as an example of “implementing security services for a mobile device” as well as the other examples cited in its analysis of element 1.4. *Id.* at 27.

Dr. Jakobsson provides testimony supporting this analysis. Jakobsson Decl. ¶¶ 104–106. Dr. Jakobsson testifies that the “processed by the security system processor to implement” limitation of claim element 19.4 is met by Groenendaal: “Each of these services is implemented by the security server processor *by processing the stored security code, security policies, and security data, as established for limitation 1.4.*” *Id.* ¶ 105 (emphasis added).

Patent Owner raises additional arguments to distinguish Groenendaal from this claim. PO Resp. 27–34. For example, Patent Owner describes the invention claimed in the ’344 patent as providing the mobile device with

IPR2021-00813  
 Patent 10,621,344 B2

“two lines of defense, one implemented by a security system and one implemented by the mobile device itself.” *Id.* at 28. According to Patent Owner, “[c]onsistent with this goal,” claims 19 and 20 of the ’344 patent require the security system to store “security information,” that is “configured to be processed by the security system’s processor to implement security services for the mobile device.” *Id.* Further, according to Patent Owner, this technique “is fundamentally different from the security system of *Groenendaal* . . . . Instead, *Groenendaal* is directed to pushing security profiles from a server to a mobile device, where the mobile device itself implements any attendant security services.” *Id.* at 28.

We do not agree with these arguments. First, as with claim element 1.4, we do not agree with Patent Owner’s claim construction that would require the security system to provide security information to the mobile units by itself. *See supra*, Sections II.C.1 & II.C.2. Furthermore, we find that Petitioner provides persuasive evidence, including expert testimony, that *Groenendaal* meets the “configured to be processed” limitation even under Patent Owner’s proposed construction. Pet. 26–27; Jakobsson Decl. ¶¶ 104–106. Petitioner demonstrates, and we find, that *Groenendaal* discloses that the security code, policy, and data provide security services to the mobile device “other than by sending a security profile.” Pet. 24–26; Pet. Reply 17–21. As Petitioner demonstrates, other examples from *Groenendaal* show the provision of “security services, *i.e.*, firewall protection, to a mobile device other than by sending it a security profile.” Pet. 24; Pet. Reply 20.

Our finding is supported by Dr. Jakobsson’s testimony that the “configured to be processed” limitation is met by *Groenendaal*. Jakobsson Decl. ¶¶ 104–106. Dr. Jakobsson testifies that in *Groenendaal*, certain

IPR2021-00813  
Patent 10,621,344 B2

security services are provided beyond those provided by sending security information to the mobile device, and “[e]ach of these services is implemented by the security server processor by processing the stored security code, security policies, and security data.” *Id.* ¶ 105.

Patent Owner contends that Dr. Jakobsson’s examples, including the firewall, do not meet the claim limitation because they are “implemented by the mobile device.” PO Resp 31. Specifically, as to the firewall example, Patent Owner contends “the enabled profile is implemented on and by the mobile device, not the server.” *Id.*

We do not agree that these arguments distinguish Groenendaal from the challenged claims. For the reasons presented *supra*, we construe “implement security services for a mobile device” in claim element 19.4 as including providing security information to the mobile device. *See supra*, Section II.C.2. We find that under this construction, Groenendaal meets this claim element, for example, by providing updated security information to the mobile devices. Pet. 6 (citing Jakobsson Decl. ¶ 57; Ex. 1001, 2:34–37). But even if we had adopted Patent Owner’s proposed construction for “implement security services for the mobile device,” we would find that Groenendaal meets this claim element, for example, in configuring or implementing firewalls for the mobile devices.

Patent Owner’s attempt to distinguish the firewall example by arguing that Groenendaal’s firewall is not implemented on the server because a gateway is involved is unavailing. *See* discussion of “additional security services” in Section II.C.4, *supra*. As discussed there, we do not agree with Patent Owner’s contention that due to the presence of the gateway, the server does not provide the claimed security services to the mobile device.

IPR2021-00813  
 Patent 10,621,344 B2

*See, e.g.*, Hearing Tr. 55:23–56:2. We find that the processing on the server to set up the firewall for the mobile device meets the claim limitation.

Jakobsson Decl. ¶ 101. As Dr Jakobsson testifies, “[e]ach of these services is implemented by the security server processor by processing the stored security code, security policies, and security data, as established for limitation 1.4.” *Id.* ¶ 105.

We therefore do not give weight to Patent Owner’s arguments or the testimony of its expert, Dr. Goodrich (Goodrich Decl. ¶¶ 82–107) attempting to rebut Dr. Jakobsson’s testimony or to distinguish Groenendaal.

Dr. Goodrich’s testimony tracks closely the arguments in Patent Owner’s responses that we find unavailing. Those arguments are based on claim constructions and other restrictions that we have rejected as not supported by the intrinsic record in Section II.C. *supra*.

We find, based on the evidence presented by Petitioner, that Groenendaal teaches claim element 19.4. Jakobsson Decl. ¶¶ 104–107.

#### 6. *Elements 1.5, 19.5*

Claims 1 and 19 also require:

the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being managed by one or more information technology (IT) administrators using an IT administrator system on a trusted enterprise network, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network.

Claim 19 recites, in addition,

the mobile device being a first computer system, the security system being a second computer system, and the IT administrator system being a third computer system, the first computer system,

IPR2021-00813

Patent 10,621,344 B2

the second computer system and the third computer system being separate computer systems,

*See* claim elements 1.5, 19.5, *supra*. Petitioner shows these elements are met by Groenendaal’s disclosure of an IT administrator using GUI 116 to manage the system’s connection, security, and firewall profiles. Pet. 28–29. Petitioner further contends, “Groenendaal also discloses the administrator manages the security manager (security code) by managing the security profiles that define its behavior, using the administrator system GUI.” *Id.* at 29–30 (citing Ex. 1003 ¶ 21). We agree with this analysis, and therefore find that the “one or more policies” referred to in the claim “can include the decisions made by the recited ‘one or more IT administrators.’” *Id.* at 30. This contention is consistent with Petitioner’s proposed claim construction which we have adopted here and in the ’368 IPR. *See supra*, Section II.C.3. Furthermore, we find, as Petitioner contends, that “Groenendaal discloses that the stored security policy, data, and code described for limitation 1.3 all are configured using input received from the IT administrator at GUI 116, which input reflects the ‘one or more policies’ in the mind of the IT administrator. The security policies, data, and code therefore are configured based on those ‘one or more policies.’” Pet. 31. We find, also, as Petitioner contends, that “Groenendaal discloses that its IT administrator implements the one or more policies discussed above.” *Id.* at 32. Thus, “the Groenendaal administrator also provides input to GUI 116 to create security profile 150 and configuration profile 152 based on the ‘one or more policies,’ as established above.” *Id.*

Finally, we find that Groenendaal discloses the “three separate computer systems” recited in claim 19: “Groenendaal’s computer 104a with GUI 116 (an ‘IT administrator system’) is a computer separate from client

IPR2021-00813  
 Patent 10,621,344 B2

computers 104b-d (mobile devices). And each of computer 104a and the mobile devices are computers separate from server 102 (security system).” *Id.* at 34 (citing Ex. 1003, Fig. 1, ¶¶ 16, 27).

Dr. Jakobsson’s testimony supports our finding that Groenendaal discloses this limitation. Jakobsson Decl. ¶¶ 106–134. Dr. Jakobsson testifies that even under Patent Owner’s claim construction analysis, Groenendaal meets this claim limitation. *Id.* ¶¶ 124–134. He testifies that the firewall and other services result from policies implemented by the administrator using the GUI. *Id.* ¶ 125 (“In particular, the GUI 116 receives and stores settings such as whether to enable a firewall, whether to enable network file sharing, and which network authentication protocol to use. The administrator finalizes and gives effect to these settings by pressing the ‘Finish’ button.”) (citations omitted). He concludes that “[t]he settings in GUI 116 therefore are an implementation of the ‘one or more policies’ described above because they become the operative policies (i.e., the policies in effect).” *Id.* at ¶ 126.

Patent Owner contends that the “one or more policies” do not encompass “mental decisions” of the IT administrator. PO Resp. 35. As we discuss *supra* in Section II.C.3, we do not agree with that contention for the reasons given there.

Patent Owner also contests Petitioner’s argument that even under Patent Owner’s construction, Groenendaal meets this limitation. PO Resp. 35. According to Patent Owner, these settings are “temporarily stored” and therefore not “put into effect” until the user presses a “Finish” or “Save” button. *Id.* We disagree with these arguments for the reasons given by Petitioner. Pet. Reply 22–23 (“[T]he settings stored in GUI 116 are an

IPR2021-00813  
 Patent 10,621,344 B2

implementation of policies because they are concrete expression of policies and are stored (at least temporarily) in the memory of laptop 104a.”).

Patent Owner acknowledges that once the settings are entered by the IP administrator, they are stored (even if temporarily) in the memory of the laptop computer. PO Resp. 35 (referring to “temporarily stored” settings in the GUI); Hearing Tr. 50:16–23. As Dr. Jakobsson testifies: “The settings in GUI 116 therefore are an implementation of the ‘one or more policies’ described above because they become the operative policies (*i.e.*, the policies in effect).” Jakobsson Decl. ¶ 126.

We find, therefore, based on the evidence presented by Petitioner, that Groenendaal teaches claim element 19.5 under either Petitioner’s or Patent Owner’s claim construction.

#### *7. Elements 1.6, 1.7, 1.8, 19.6, 19.7, 19.8*

Petitioner provides similar element-by-element analyses for the remaining limitations of claim 1 and claim 19. Pet. 38–47. Patent Owner does not challenge this analysis. We find, based on the evidence presented by Petitioner, that Groenendaal teaches claim elements 1.6–1.8 and 19.6–19.8. Jakobsson Decl. ¶¶ 135–149.

#### *8. Summary Claims 1 and 19*

We have considered the entire record including Petitioner’s analysis of claims 1 and 19 in relation to Groenendaal and the arguments presented by Patent Owner. Considering the evidence presented in the Petition and Patent Owner’s responses, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 1 and 19 would have been obvious in light of Groenendaal.

IPR2021-00813  
Patent 10,621,344 B2

*C. Claims 10 and 20*

Petitioner’s analysis of claims 10 and 20 tracks its analysis of claims 1 and 19. Pet. 53–55. Patent Owner does not specifically address claim 10 or distinguish between claims 19 and 20 in its response. PO Resp. 28–36. Accordingly, for the reasons given above for claims 1 and 19, we determine that Petitioner has demonstrated by a preponderance of the evidence that claims 10 and 20 would have been obvious in light of Groenendaal. Jakobsson Decl. ¶¶ 160–167.

*D. Claims 2–9 and 11–18*

Claims 2–9 depend directly from claim 1. Claims 11–18 depend directly from claim 10. The two sets of dependent claims are parallel, and each set provides the same additional features to the claims from which they depend. Claim 2, for example, specifies that the security system is “on a separate appliance removably coupled to the mobile device.” Ex. 1001, 16:1–3. Claim 11 requires “coupling the security system to the mobile device.” *Id.* at 17:10–12. Petitioner provides an element-by-element analysis of each dependent claim in relation to Groenendaal. Pet. 47–52, 55–56.

Patent Owner does not respond further to Petitioner’s analysis of these dependent claims with the exception of claims 8 and 17. PO Resp. 37–39; PO Sur-reply 22–24. Those claims each recite that “the security code, the security policy, and the security data are *configured to mirror* security policies of a gateway on the trusted enterprise network.” Ex. 1001, 16:20–23, 17:32–35 (emphases added).

Patent Owner contends that Groenendaal “does not teach or suggest this feature of the Challenged Claims.” PO Resp. 38 (citing Goodrich Decl.

IPR2021-00813  
 Patent 10,621,344 B2

¶¶ 108–117); PO Sur-reply 22. As explained by Patent Owner, “[t]he specification [of the ’344 patent] explains that the enterprise’s gateway (which is on the *enterprise[’]s network security system*) pushes security policies and data onto the claimed *security system* . . . . In this manner, the security system is ‘configured to mirror security policies of a gateway.’” PO Sur-reply 22. Patent Owner continues, “Groenendaal does just the opposite: at best, policies of a remote gateway are configured to mirror those of server 102.” *Id.* at 23.

We do not agree with this argument by Patent Owner attempting to distinguish Groenendaal because the argument is not supported by the language of the claims. We find, as Petitioner explains, that claims 8 and 17 do not impose an order of operations:

Groenendaal discloses that policies are pushed from the Groenendaal server to the Groenendaal gateway. Patent Owner argues that that disclosure doesn’t satisfy this limitation because the policies have to be on the gateway first and are copied to the server, not vice versa. But *the claim language doesn’t require an order of operations. The claim language includes the state of being mirrored.*

Hearing Tr. 22:20–23 (emphasis added). Petitioner relies on the inclusion in the claims of the term “configured”: “After one has configured a server and a gateway to have the same policies they are configured to mirror each other. They do mirror each other.” *Id.* at 23:1–3. We agree with Petitioner’s reasoning that the claims do not impose an order, and we therefore find that Groenendaal teaches the “configured to mirror” limitation of claims 8 and 17. We further determine for the reasons given by Petitioner that claims 2–9 and 11–18 would have been obvious over Groenendaal. Jakobsson Decl. ¶¶ 150–159, 168–175.

IPR2021-00813  
Patent 10,621,344 B2

#### IV. CONCLUSION

For the foregoing reasons, we determine Petitioner has demonstrated by a preponderance of the evidence that all challenged claims of the '344 patent would have been obvious and are, therefore, unpatentable. Our conclusions are summarized in the following table.

<b>Claims</b>	<b>35 U.S.C. §</b>	<b>Reference(s)/ Basis</b>	<b>Claims Shown Unpatentable</b>	<b>Claims Not Shown Unpatentable</b>
1–20	103(a)	Groenendaal	1–20	
<b>Overall Outcome</b>			1–20	

#### V. ORDER

For the foregoing reasons, it is  
ORDERED that claims 1–20 of the '344 patent are unpatentable; and  
FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.<sup>8</sup>

---

<sup>8</sup> Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

IPR2021-00813  
Patent 10,621,344 B2

PETITIONER:

Robert Buergi  
James Heintz  
DLA Piper LLR (US)  
robert.buergi@dlapiper.com  
jim.heintz@dlapiper.com

PATENT OWNER:

James Hannah  
Jeffrey Price  
Jenna Fuller  
KRAMER LEVIN NAFTALIS &  
FRANKEL LLP  
jhannah@kramerlevin.com  
jprice@kramerlevin.com  
jfuller@kramerlevin.com



US010621344B2

(12) **United States Patent**  
**Touboul**

(10) **Patent No.: US 10,621,344 B2**

(45) **Date of Patent: \*Apr. 14, 2020**

(54) **SYSTEM AND METHOD FOR PROVIDING  
NETWORK SECURITY TO MOBILE  
DEVICES**

(71) Applicant: **CUPP Computing AS**, Oslo (NO)

(72) Inventor: **Shlomo Touboul**, Kefar Haim (IL)

(73) Assignee: **CUPP Computing AS**, Oslo (NO)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/656,358**

(22) Filed: **Oct. 17, 2019**

(65) **Prior Publication Data**

US 2020/0057852 A1 Feb. 20, 2020

**Related U.S. Application Data**

(63) Continuation of application No. 16/573,877, filed on Sep. 17, 2019, which is a continuation of application (Continued)

(51) **Int. Cl.**  
**G06F 21/00** (2013.01)  
**G06F 21/56** (2013.01)  
(Continued)

(52) **U.S. Cl.**  
CPC ..... **G06F 21/562** (2013.01); **H04L 63/02** (2013.01); **H04L 63/0263** (2013.01);  
(Continued)

(58) **Field of Classification Search**  
CPC ..... G06F 21/56; G06F 21/00; G06F 21/50;  
H04L 63/02; H04L 63/0245; H04L  
63/0227

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

H001944 H \* 2/2001 Cheswick ..... 726/11  
H0001944 H 2/2001 Cheswick

(Continued)

FOREIGN PATENT DOCUMENTS

WO 2000078008 12/2000  
WO 2004030308 4/2004

(Continued)

OTHER PUBLICATIONS

Breedon II, John et al., "A Hardware Firewall You Take With You," Government Computer News, located at <http://gcen.com/Articles/2005/06/01/A-hardware-firewall-you-take-with-you.aspx?p=1>, Jun. 1, 2005.

(Continued)

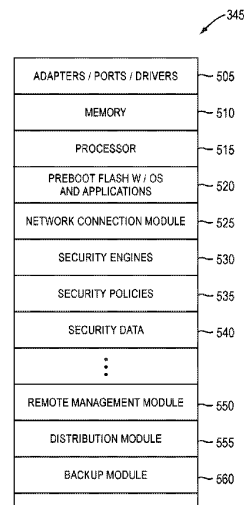
*Primary Examiner* — Izunna Okeke

(74) *Attorney, Agent, or Firm* — Sheppard, Mullin, Richter & Hampton LLP

(57) **ABSTRACT**

A small piece of hardware connects to a mobile device and filters out attacks and malicious code. Using the piece of hardware, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise. In one embodiment, a mobile security system includes a connection mechanism for connecting to a data port of a mobile device and for communicating with the mobile device; a network connection module for acting as a gateway to a network; a security policy for determining whether to forward content intended for the mobile device to the mobile device; and a security engine for executing the security policy.

**20 Claims, 10 Drawing Sheets**



## US 10,621,344 B2

Page 2

## Related U.S. Application Data

No. 16/144,408, filed on Sep. 27, 2018, now Pat. No. 10,417,421, which is a continuation of application No. 15/689,795, filed on Aug. 29, 2017, now Pat. No. 10,089,462, which is a continuation of application No. 15/586,176, filed on May 3, 2017, now Pat. No. 9,747,444, which is a continuation of application No. 15/352,553, filed on Nov. 15, 2016, now Pat. No. 9,781,164, which is a continuation of application No. 14/092,756, filed on Nov. 27, 2013, now Pat. No. 9,497,622, which is a continuation of application No. 13/735,836, filed on Jan. 7, 2013, now Pat. No. 8,627,452, which is a continuation of application No. 11/376,919, filed on Mar. 15, 2006, now Pat. No. 8,381,297.	8,904,523 B2	12/2014	Gordon
	8,978,132 B2	3/2015	Henry
	9,202,070 B2	12/2015	Rajakarunanayake
	9,438,631 B2	9/2016	Bettini
	9,565,202 B1	2/2017	Kindlund
	9,762,614 B2	9/2017	Ely
	9,832,603 B2	11/2017	Schlaupitz
	9,847,020 B2	12/2017	Davis
	9,910,979 B2	3/2018	Ben-Haim
	10,291,656 B2	5/2019	Ely
	2001/0014102 A1	8/2001	Mattingly
	2002/0111824 A1	8/2002	Grainger
	2003/0046397 A1	3/2003	Trace
	2003/0055994 A1	3/2003	Herrmann
	2003/0070084 A1	4/2003	Satoomaa
	2003/0097431 A1	5/2003	Dill
	2003/0110391 A1	6/2003	Wolff
	2003/0126468 A1	7/2003	Markham
	2003/0131245 A1	7/2003	Linderman
	2003/0142683 A1	7/2003	Lam
	2003/0224758 A1	12/2003	O'Neill
	2003/0229808 A1	12/2003	Heintz
	2004/0003262 A1	1/2004	England
	2004/0019656 A1	1/2004	Smith
	2004/0064575 A1	4/2004	Rasheed
	2004/0085944 A1	5/2004	Boehm
	2004/0093520 A1	5/2004	Lee
	2004/0123153 A1*	6/2004	Wright ..... G06F 21/32 726/1
(60) Provisional application No. 60/750,326, filed on Dec. 13, 2005.			
(51) <b>Int. Cl.</b>			
<b>H04L 29/06</b> (2006.01)			
<b>H04W 12/12</b> (2009.01)			
<b>H04W 12/00</b> (2009.01)			
(52) <b>U.S. Cl.</b>			
CPC ..... <b>H04L 63/145</b> (2013.01); <b>H04L 63/1416</b> (2013.01); <b>H04L 63/1441</b> (2013.01); <b>H04L 63/20</b> (2013.01); <b>H04W 12/00</b> (2013.01); <b>H04W 12/12</b> (2013.01); <b>H04W 12/1208</b> (2019.01)			
(56) <b>References Cited</b>			
U.S. PATENT DOCUMENTS			
6,286,087 B1	9/2001	Ito	
6,466,779 B1	10/2002	Moles	
6,772,345 B1	8/2004	elShetty	
6,813,682 B2	11/2004	Bress	
7,036,143 B1	4/2006	Leung	
7,065,644 B2	6/2006	Daniell	
7,069,330 B1	6/2006	McArdle	
7,076,690 B1	7/2006	Todd	
7,086,089 B2	8/2006	Hrastar	
7,131,141 B1	10/2006	Blewett	
7,168,089 B2	1/2007	Nguyen	
7,184,554 B2	2/2007	Freese	
7,197,638 B1	3/2007	Grawrock	
7,283,542 B2	10/2007	Mitchell	
7,353,533 B2	4/2008	Wright	
7,359,983 B1	4/2008	Maufer	
7,360,242 B2	4/2008	Syvanne	
7,418,253 B2	8/2008	Kavanagh	
7,529,932 B1	5/2009	Haustein	
7,539,828 B2	5/2009	Lomnes	
7,657,941 B1	2/2010	Zaitsev	
7,665,137 B1	2/2010	Barton	
7,818,803 B2	10/2010	Gordon	
7,894,480 B1	2/2011	Wang et al.	
7,908,476 B2	3/2011	Kandasamy	
7,971,258 B1	6/2011	Liao	
7,984,479 B2	7/2011	Brabson	
7,992,199 B1	8/2011	Winick	
8,180,654 B2	5/2012	Berkman	
8,218,449 B2	7/2012	Taylor	
8,218,558 B2	7/2012	Tan	
8,234,261 B2	7/2012	Monahan	
8,239,531 B1	8/2012	Bellovin	
8,266,670 B1	9/2012	Merkow	
8,321,934 B1	11/2012	Cooley	
8,402,528 B1*	3/2013	McCorkendale ..... G06F 8/65 726/11	
8,495,700 B2	7/2013	Shahbazi	
8,631,488 B2	1/2014	Oz	
	5/2004	Aroya	
	10/2004	Freund	
	10/2004	Moreton	
	10/2004	Gbadegesin	
	11/2004	Cox	
	3/2005	Wright	
	4/2005	Hearn	
	5/2005	Ryan	
	5/2005	Hesslink	
	5/2005	Song	
	7/2005	Corbett	
	9/2005	Buniatyan	
	11/2005	Plehn	
	11/2005	Groenendaal	
	12/2005	Cromer	
	12/2005	Baxter	
	2/2006	Bridgelall	
	2/2006	Rozman	
	2/2006	Rao	
	3/2006	Manning	
	3/2006	Burshan	
	3/2006	Petrov	
	3/2006	Sobel et al.	
	4/2006	Thomas	
	4/2006	Bertman	
	4/2006	Thomas	
	4/2006	Thomas	
	7/2006	Zhao	
	8/2006	Zaheer	
	9/2006	Garg et al.	
	10/2006	Stevens	
	10/2006	Achanta	
	10/2006	Toda	
	12/2006	Bowler	
	1/2007	Durham	
	1/2007	Rowett	
	3/2007	Eisink	
	3/2007	Hoover	
	4/2007	Fruhauf	
	5/2007	Wood	
	5/2007	King	
	5/2007	Soni et al.	
	5/2007	Adams	
	5/2007	Crawford	
	5/2007	Mock	
	6/2007	Safa	
	6/2007	Kamat	
	6/2007	Nicodemus	
	6/2007	Nicodemus	
	7/2007	Belali et al.	

TREND MICRO

EXHIBIT 1001 - PAGE 2

## US 10,621,344 B2

Page 3

(56)

## References Cited

## U.S. PATENT DOCUMENTS

2007/0192500 A1 8/2007 Lum  
 2007/0192854 A1 8/2007 Kelley  
 2007/0199060 A1 8/2007 Touboul  
 2007/0199061 A1 8/2007 Byres  
 2007/0209067 A1 9/2007 Fogel  
 2007/0214369 A1 9/2007 Roberts  
 2007/0233842 A1 10/2007 Roberts  
 2007/0240217 A1 10/2007 Tuvell  
 2007/0261112 A1 11/2007 Todd  
 2007/0266265 A1 11/2007 Zmudzinski  
 2007/0281664 A1 12/2007 Kaneko  
 2007/0294744 A1\* 12/2007 Alessio ..... H04L 63/20  
 2008/0034419 A1 2/2008 Mullick  
 2008/0066148 A1 3/2008 Lim  
 2008/0083030 A1 4/2008 Durham  
 2008/0083037 A1 4/2008 Kruse  
 2008/0084799 A1 4/2008 Repasi  
 2008/0098478 A1 4/2008 Vaidya  
 2008/0109871 A1 5/2008 Jacobs  
 2008/0114990 A1 5/2008 Hilbert  
 2008/0134163 A1 6/2008 Golde  
 2008/0141349 A1 6/2008 Lyle  
 2008/0165957 A1 7/2008 Kandasamy et al.  
 2008/0201264 A1 8/2008 Brown  
 2008/0235755 A1 9/2008 Blaisdell  
 2008/0282337 A1 11/2008 Crawford  
 2008/0307240 A1 12/2008 Dahan  
 2009/0019223 A1 1/2009 Lection  
 2009/0054075 A1 2/2009 Boejer  
 2009/0106556 A1 4/2009 Hamid  
 2009/0143057 A1 6/2009 Arun et al.  
 2009/0165132 A1 6/2009 Jain  
 2009/0249465 A1 10/2009 Touboul  
 2009/0253454 A1 10/2009 Sampson  
 2009/0254993 A1 10/2009 Leone  
 2010/0064341 A1 3/2010 Aldera  
 2010/0186093 A1 7/2010 Aussel  
 2010/0195833 A1 8/2010 Priestley  
 2010/0218012 A1 8/2010 Joseph  
 2010/0225493 A1 9/2010 Zishaan  
 2010/0242109 A1 9/2010 Lee  
 2010/0251369 A1 9/2010 Grant  
 2010/0269172 A1 10/2010 Xie  
 2010/0333088 A1 12/2010 Rogel  
 2011/0023118 A1 1/2011 Wright  
 2011/0154443 A1 6/2011 Thakur  
 2011/0154477 A1 6/2011 Parla  
 2011/0182180 A1 7/2011 Riddle  
 2011/0264931 A1 10/2011 Chang  
 2011/0268106 A1 11/2011 Dalton, Jr.  
 2011/0269397 A1 11/2011 Bella  
 2012/0005756 A1 1/2012 Hoefelmeyer  
 2012/0030750 A1 2/2012 Bhargava et al.  
 2012/0054744 A1 3/2012 Singh  
 2012/0084831 A1 4/2012 Hu  
 2012/0110320 A1 5/2012 Kumar  
 2012/0110331 A1 5/2012 Falk  
 2012/0149350 A1 6/2012 Fan  
 2012/0173609 A1 7/2012 Kulaga  
 2012/0185846 A1 7/2012 Recio  
 2012/0216273 A1 8/2012 Rolette  
 2012/0233695 A1 9/2012 Mahaffey  
 2012/0239739 A1 9/2012 Manglik  
 2012/0240183 A1 9/2012 Sinha  
 2012/0240236 A1 9/2012 Wyatt  
 2012/0303971 A1 11/2012 Palka  
 2013/0031601 A1 1/2013 Bott  
 2013/0074144 A1 3/2013 Narayanaswamy  
 2013/0091534 A1 4/2013 Gilde  
 2013/0097659 A1 4/2013 Das  
 2013/0097660 A1 4/2013 Das  
 2014/0032314 A1 1/2014 Gieseke  
 2014/0058679 A1 2/2014 Varoglu  
 2014/0317679 A1 10/2014 Wade

2016/0105847 A1 4/2016 Smith  
 2016/0234204 A1 8/2016 Rishi  
 2017/0039367 A1 2/2017 Ionescu  
 2017/0103647 A1 4/2017 Davis

## FOREIGN PATENT DOCUMENTS

WO 2006069041 6/2006  
 WO 2007110094 10/2007  
 WO 2008154726 12/2008  
 WO 2009004452 1/2009

## OTHER PUBLICATIONS

Claessens, Joris et al., "(How) Can Mobile Agents Do Secure Electronic Transactions on Mobile Hosts? A Survey of the Security Issues and the Current Solutions," ACM Transactions on Internet Technology, vol. 3, No. 1, pp. 28-48, Feb. 2003.  
 CyberGuard Corporation, "Model 1: Wireless Mobile Security Appliance," located at <http://support2.cyberguard.com/products/oem/model1.htm>, 2005.  
 Entry, Inc., "CyberGuard Develops a Custom Mobile Security Appliance," SecurityProNews, located at <http://www.securitypronews.com/news/securitynews/spn-45-20041007CyberGuardDevelop...>, Oct. 7, 2004.  
 Fielding, R. et al., "Hypertext Transfer Protocol—HTTP/1.1," I.E.T.F. Network Working Group, RFC 2616, Jun. 1999.  
 Hall, Marty, "Core Web Programming: Chapter 16—The Hypertext Transfer Protocol," Prentice Hall PTR, ISBN 0-13-625666-X, pp. 867-911, Dec. 1997.  
 Hall, Marty, "More Servlets and JavaServer Pages: Chapter 2—A Fast Introduction to Basic Servlet Programming," Prentice Hall PTR, ISBN 0-13-067614-4, pp. 34-118, Dec. 1997.  
 Henmi, Anne et al., "Firewall Policies and VPN Configurations," Syngress Publishing, Inc., ISBN 1-59749-088-1, pp. 99-133, 291-313, Dec. 2006.  
 Jakobsson, Markus, "Invasive Browser Sniffing and Countermeasures," Proceedings of the 15th International Conference on World Wide Web, pp. 523-532, May 23, 2006.  
 Kent, S. et al., "Security Architecture for the Internet Protocol," I.E.T.F. Network Working Group, RFC 4301, pp. 10-11, Dec. 2005.  
 Lee, Henry C.J. et al., "Port Hopping for Resilient Networks," IEEE 60th Vehicular Technology Conference (VTC2004), Sep. 26, 2004.  
 O'Brien, Kevin J., "Microsoft Hit by Antitrust Complaint for Browser," The International Herald Tribune, Dec. 14, 2007.  
 PMC-Sierra, Inc., "MSP8120 Multi-Service Security Processor," Product Brief, 2007.  
 Prevelakis, Vassilis et al., "Drop-In Security for Distributed and Portable Computing Elements," Internet Research: Electronic Networking, Applications and Policy, vol. 13, No. 2, pp. 107-115, located at <http://www.cs.columbia.edu/~angelos/Papers/InternetResearch-Final.pdf>, 2003.  
 Sen, Subhabrata et al., "Accurate, Scalable In-Network, Identification of P2P Traffic Using Application Signatures," Proceedings of the 13th International Conference on World Wide Web, pp. 512-521, May 17, 2004.  
 Shreeve, Jimmy Lee, "Hasta la Vista, Microsoft!: It's Faster than Windows, It Fights Viruses—and It's Free," Independent Extra, Aug. 29, 2007.  
 Shuler, Rus, "How Does the Internet Work," white paper, 2002 [retrieved online at <https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm> on Dec. 11, 2018].  
 Srisuresh, P. et al., "IP Network Address Translator (NAT) Terminology and Considerations," I.E.T.F. Network Working Group, RFC 2663, Aug. 1999.  
 Srisuresh, P. et al., "Traditional IP Network Address Translator (Traditional NAT)," I.E.T.F. Network Working Group, RFC 3022, Jan. 2001.  
 WatchGuard Technologies, Inc., "Mobile User VPN and PPTP," Internet Security Handbook, copyright 1998-2001, pp. 1-2, located at <http://www.watchguard.com/help/Iss/41/handbook/vpn3.htm>, believe published Jun. 5, 2003.

**US 10,621,344 B2**

Page 4

(56)

**References Cited****OTHER PUBLICATIONS**

World Wide Web Consortium (W3C), "HTTP Request Fields," May 3, 1994 [retrieved online at <https://web.archive.org/web/20060110150527/http://www.w3.org:80/Protocols/HTTP/HTREQ-Headers.html> on Jan. 24, 2019].

ZyXEL Communications Corp., "ZyXEL Releases Worlds First Palm-Sized Portable Personal Firewall for Ultimate Security: ZyWALL P1 Pushes Network Security to the End-Point PC's with Minimum Administration Effort," ZyXEL News, located at <http://globat.zyxel.com/news/press.php?indexflag=20050310013432>, Mar. 8, 2005.

European Patent Application No. 06821641.5, Examination Report dated Dec. 16, 2016.

European Patent Application No. 06821641.5, Search Report dated May 17, 2011.

European Patent Application No. 08847968.8, Search Report dated Oct. 25, 2011.

European Patent Application No. 13845746.0, Search Report dated Jun. 7, 2016.

International Application No. PCT/IL2006/001428, International Search Report and Written Opinion dated Jul. 15, 2008.

International Application No. PCT/IL2008/000740, International Search Report and Written Opinion dated Nov. 5, 2008.

International Application No. PCT/US2008/055942, International Search Report and Written Opinion dated Apr. 6, 2009.

International Application No. PCT/US2009/065204, International Search Report and Written Opinion dated Jan. 13, 2010.

International Application No. PCT/US2013/064161, International Search Report and Written Opinion dated Apr. 18, 2014.

International Application No. PCT/US2014/045826, International Search Report and Written Opinion dated Oct. 30, 2014.

International Application No. PCT/US2015/015970, International Search Report and Written Opinion dated May 28, 2015.

Decision—Institution of Inter Partes Review of U.S. Pat. No. 9,781,164 entered Jun. 25, 2019 (28 pages).

Liang et al., "Passive Wake-up Scheme for Wireless Sensor Networks", Second International Conference on Innovative Computing, Information and Control, 2007, 4 pages.

Lim et al., "Adaptive power controllable retrodirective array system for wireless sensor server applications", IEEE Transactions on Microwave Theory and Techniques, vol. 53, No. 12, Dec. 2005, pp. 3735-3743.

\* cited by examiner

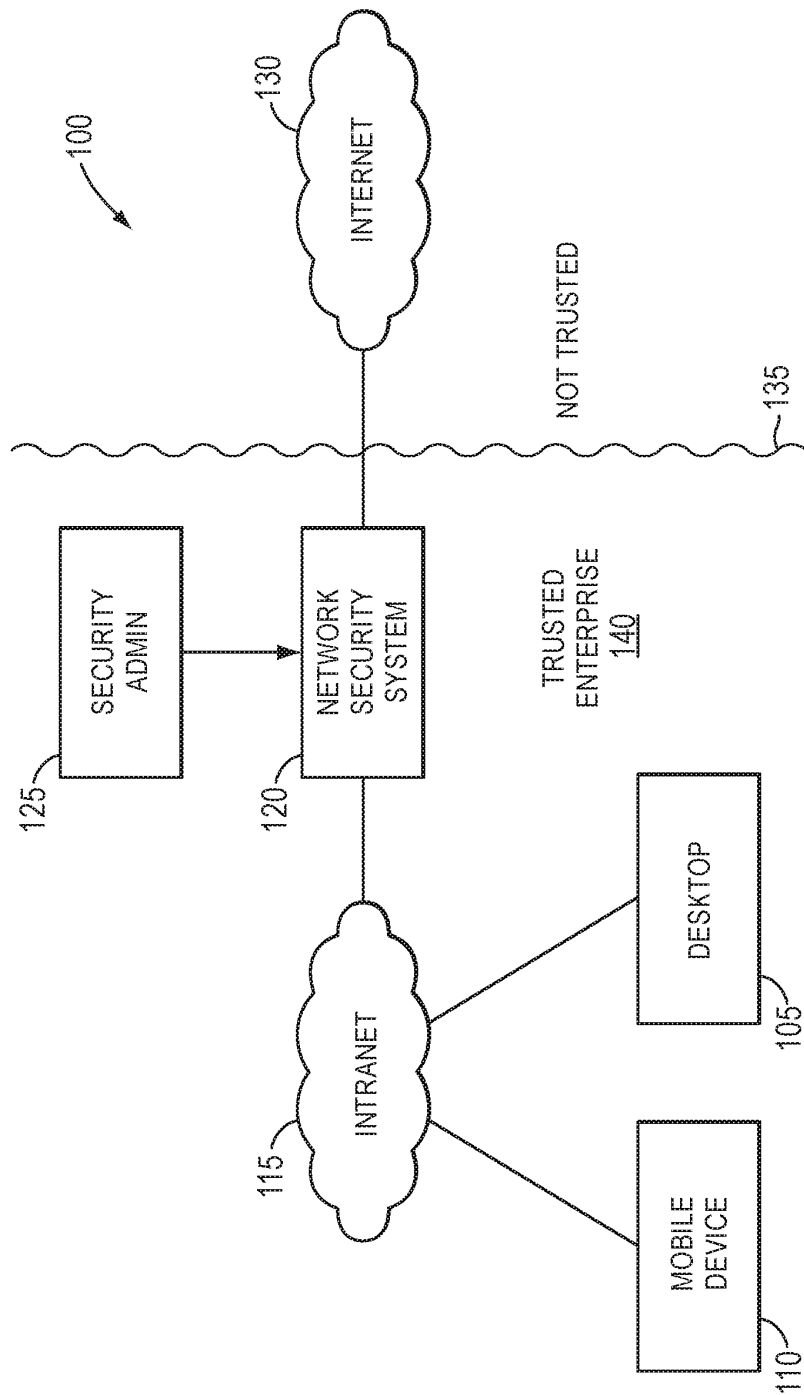


FIG. 1  
(PRIOR ART)

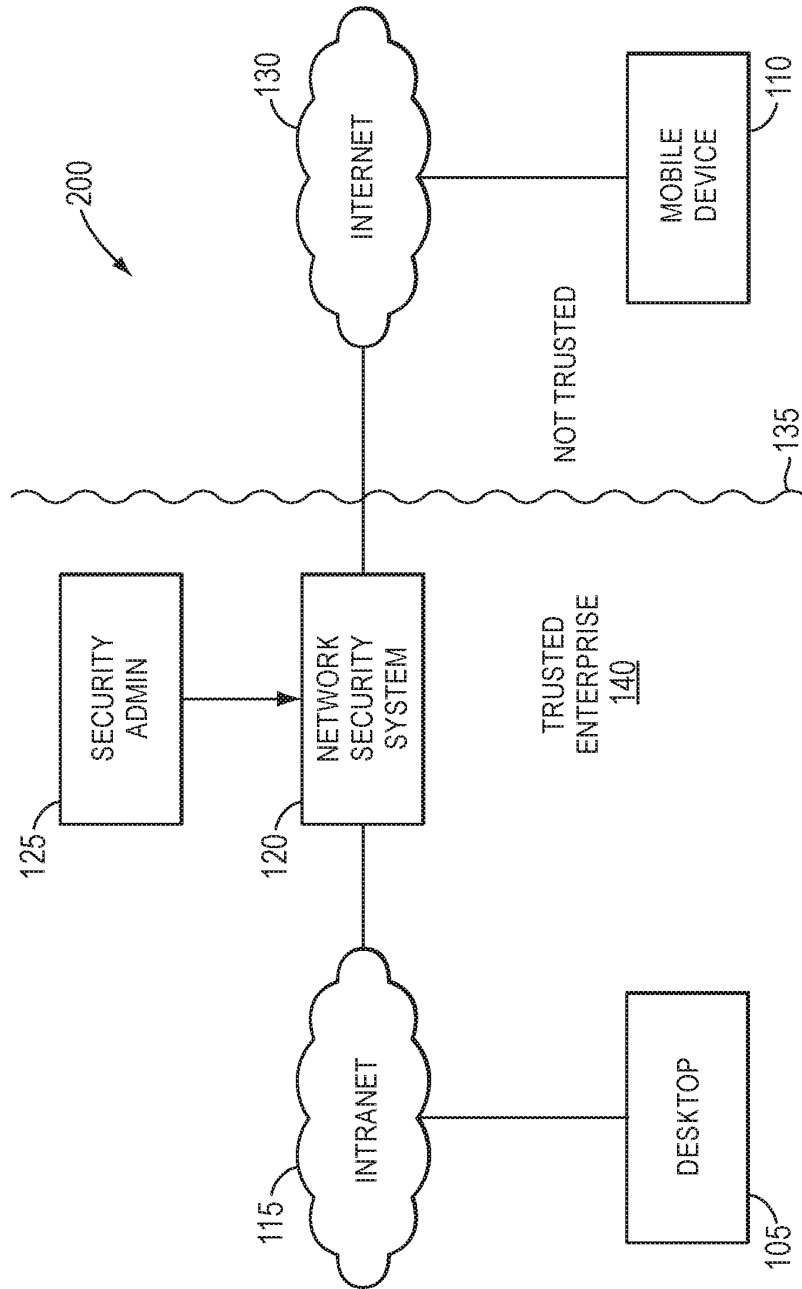


FIG. 2  
(PRIOR ART)

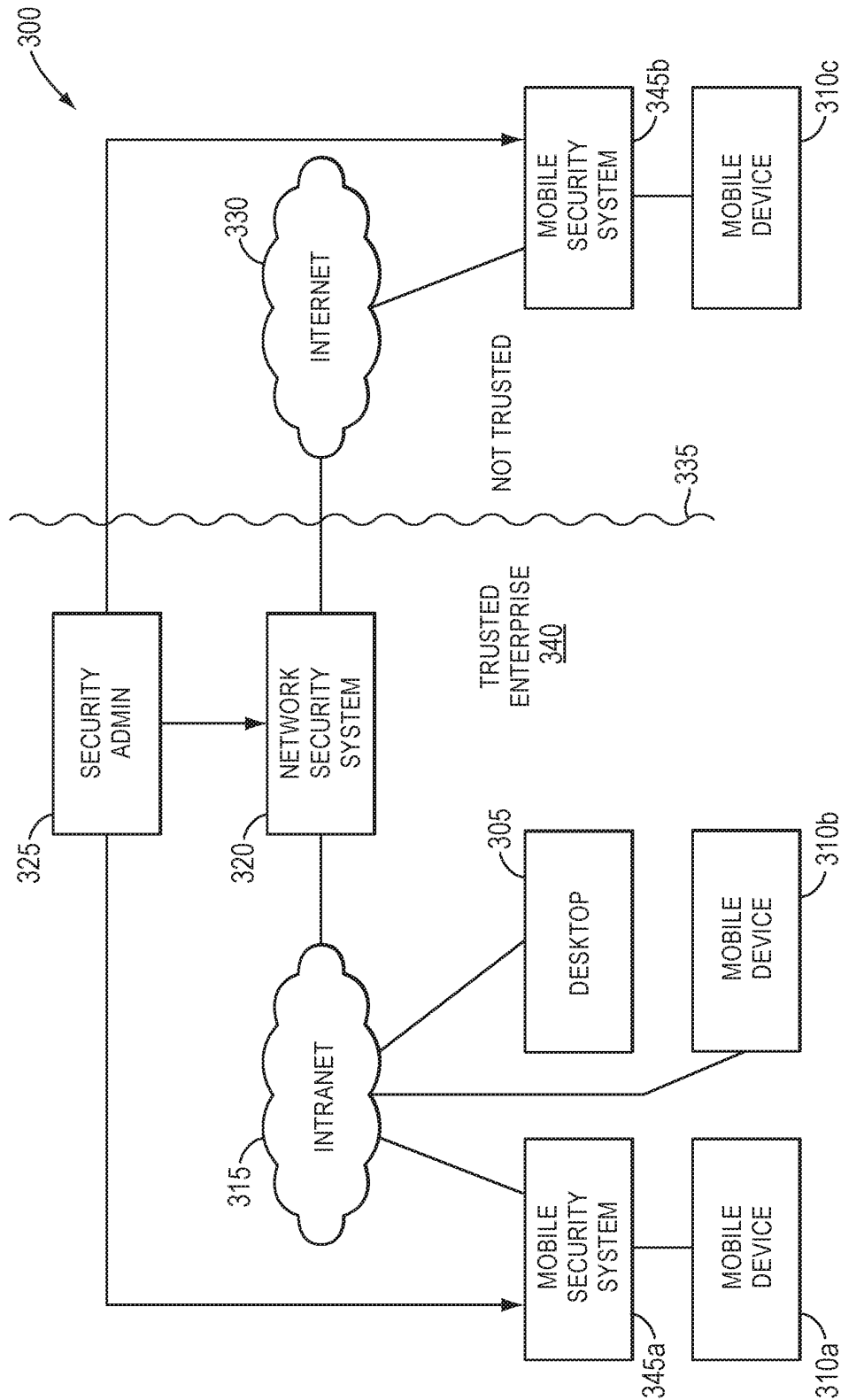


FIG. 3

U.S. Patent

Apr. 14, 2020

Sheet 4 of 10

US 10,621,344 B2

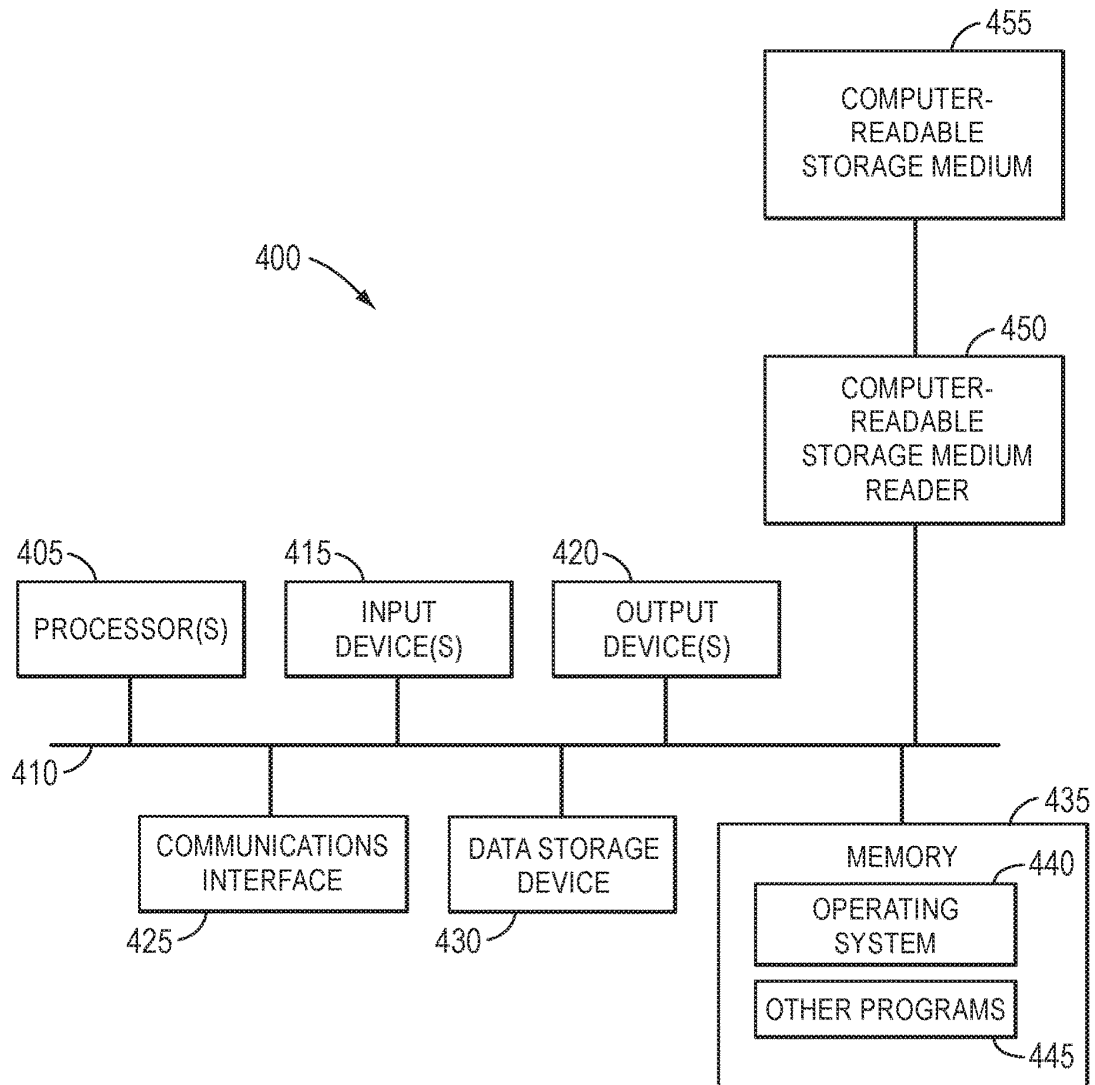


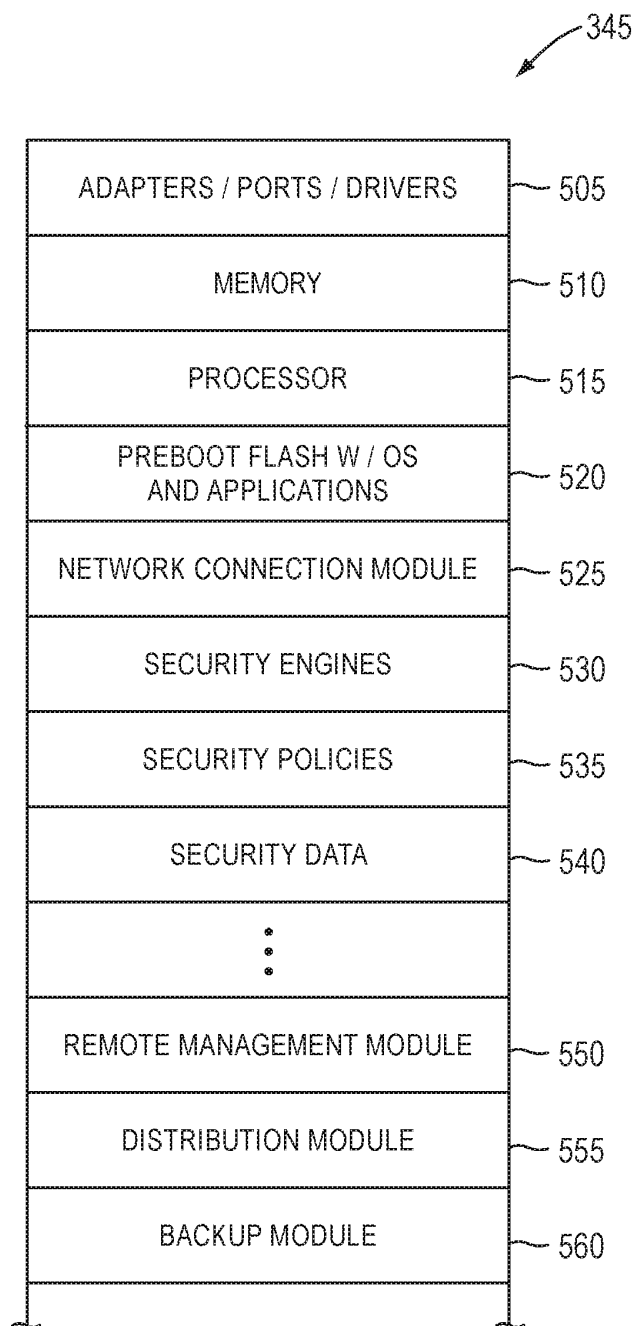
FIG. 4

**U.S. Patent**

**Apr. 14, 2020**

**Sheet 5 of 10**

**US 10,621,344 B2**



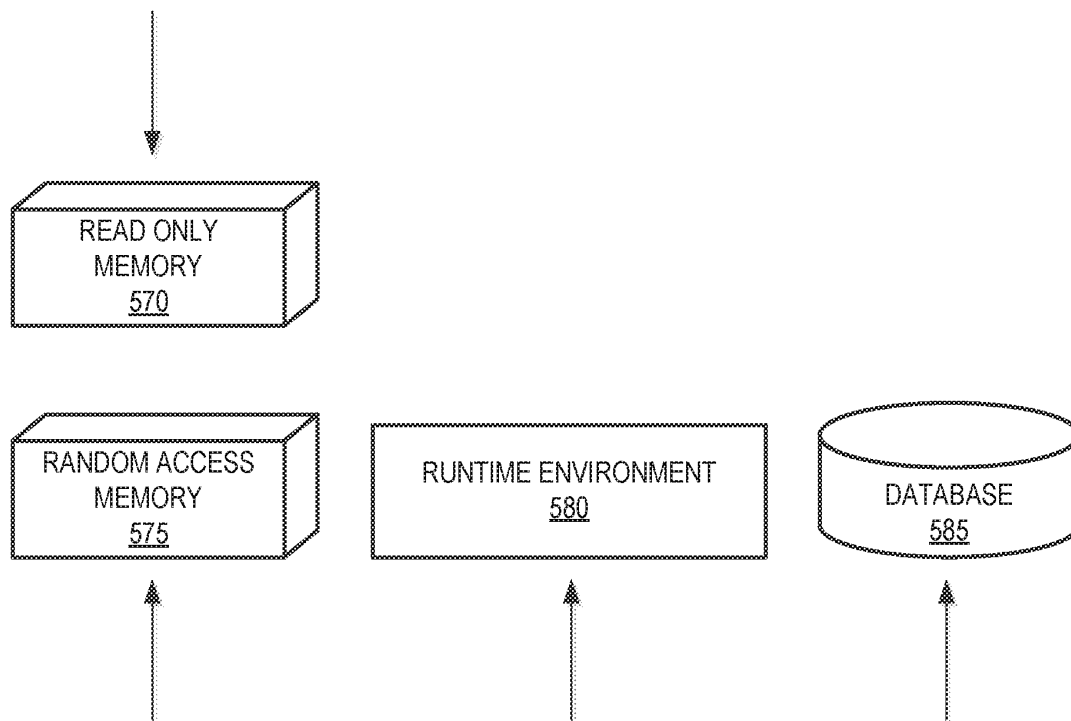
**FIG. 5**

**U.S. Patent**

**Apr. 14, 2020**

**Sheet 6 of 10**

**US 10,621,344 B2**



**FIG. 5A**

U.S. Patent

Apr. 14, 2020

Sheet 7 of 10

US 10,621,344 B2

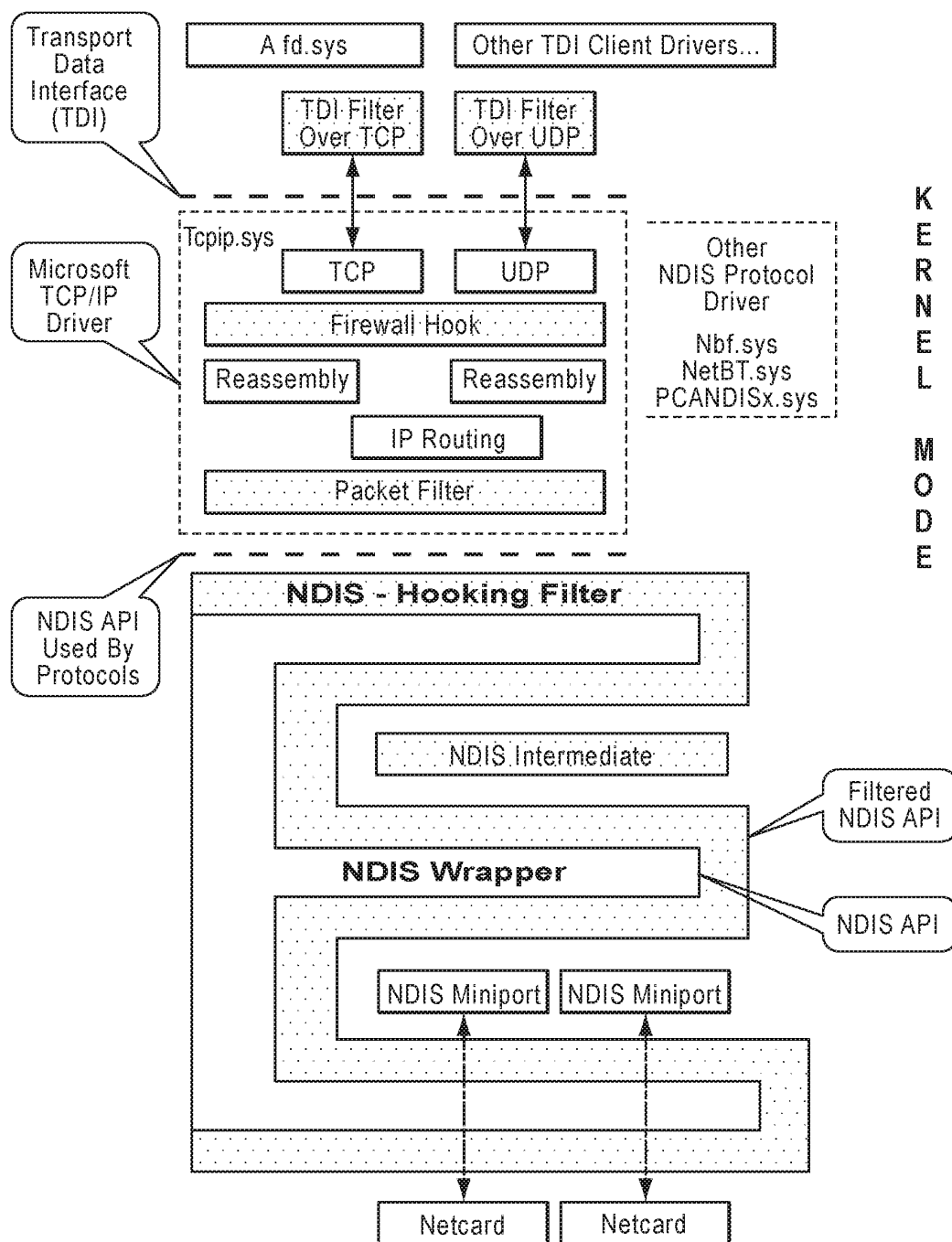


FIG. 6

U.S. Patent

Apr. 14, 2020

Sheet 8 of 10

US 10,621,344 B2

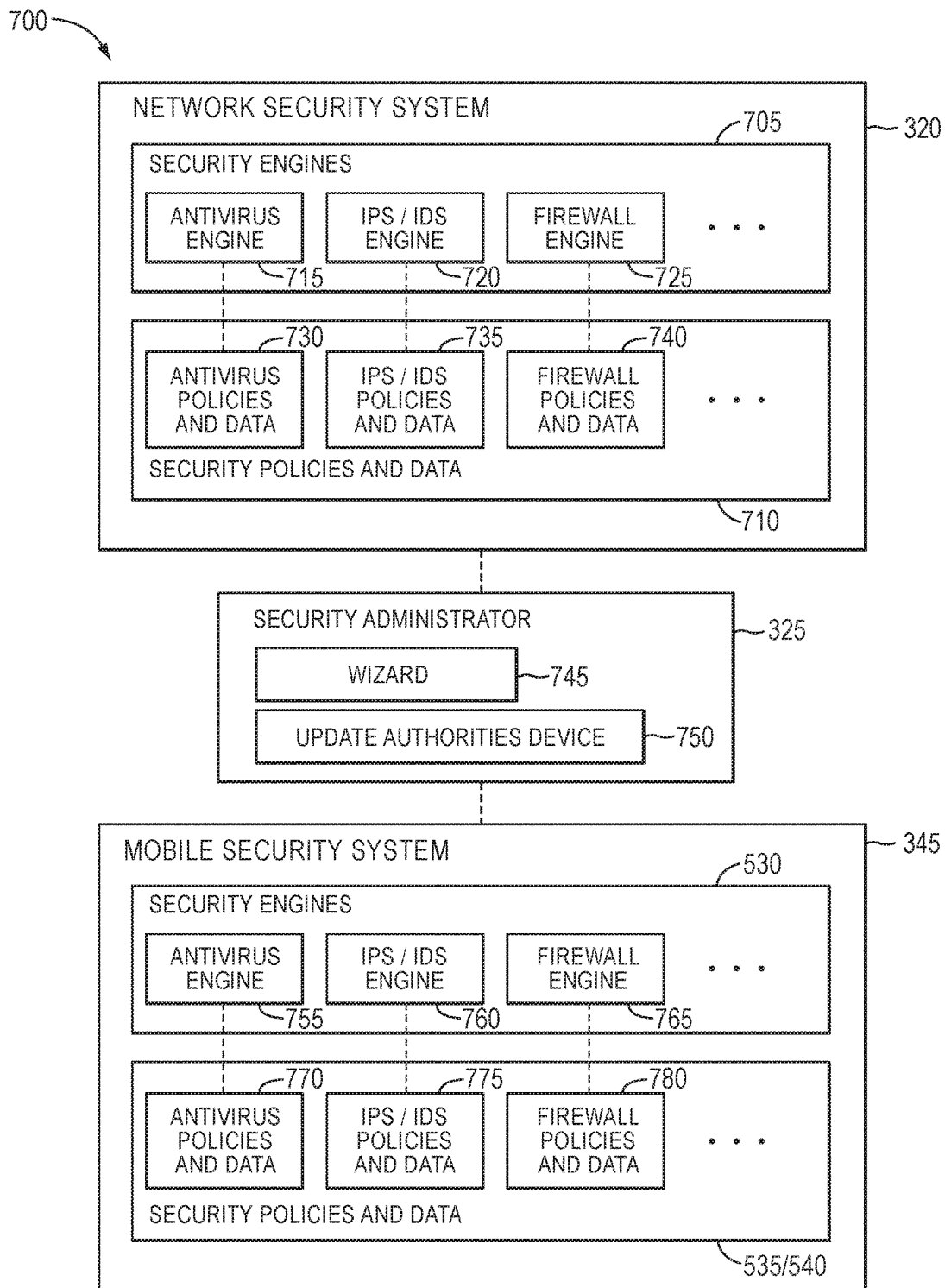


FIG. 7

U.S. Patent

Apr. 14, 2020

Sheet 9 of 10

US 10,621,344 B2

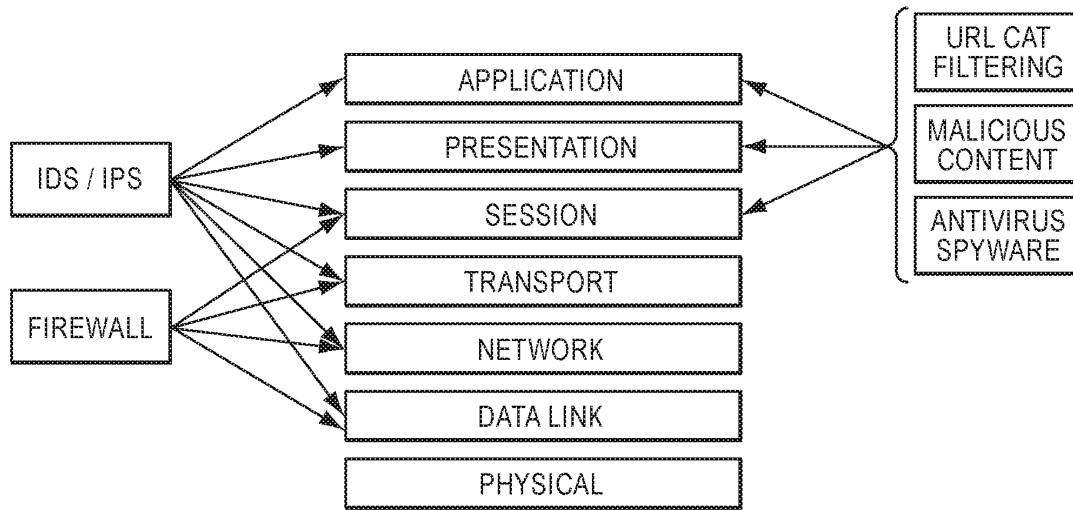


FIG. 8

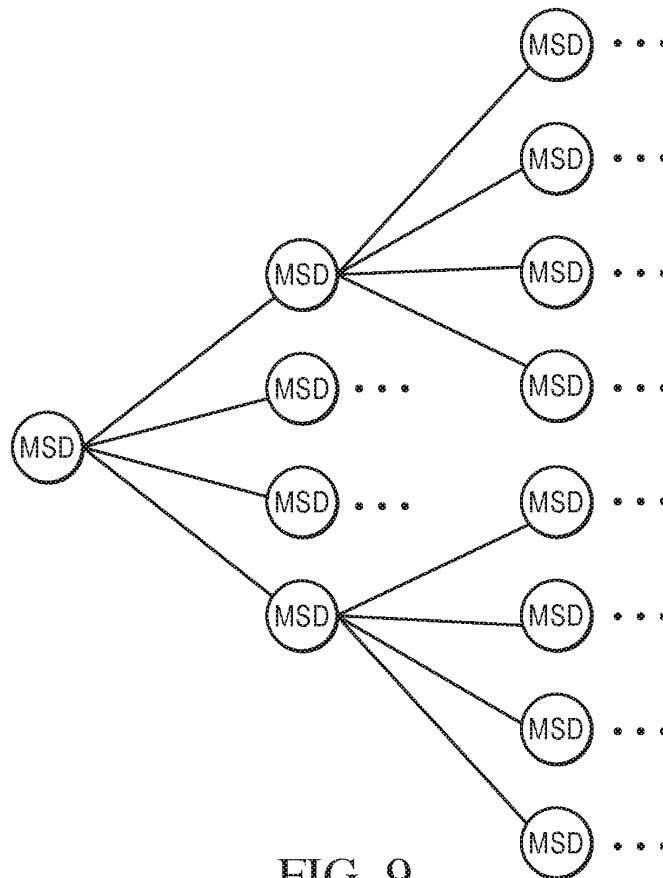


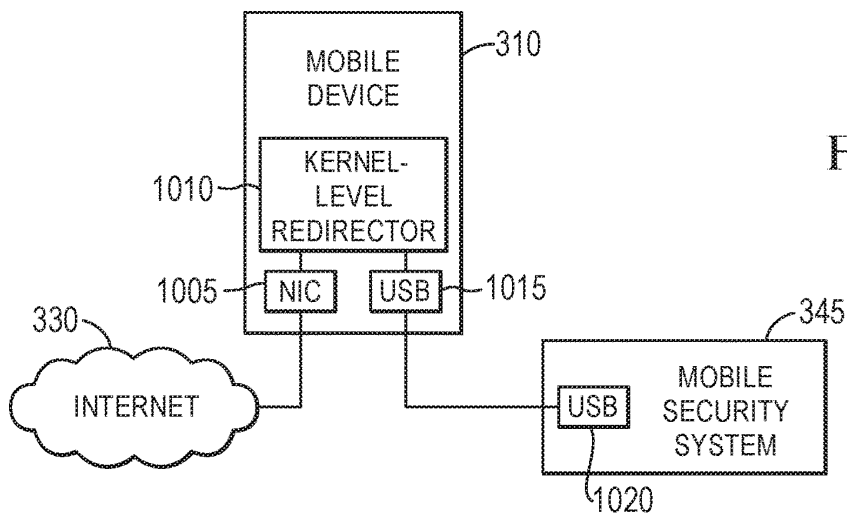
FIG. 9

**U.S. Patent**

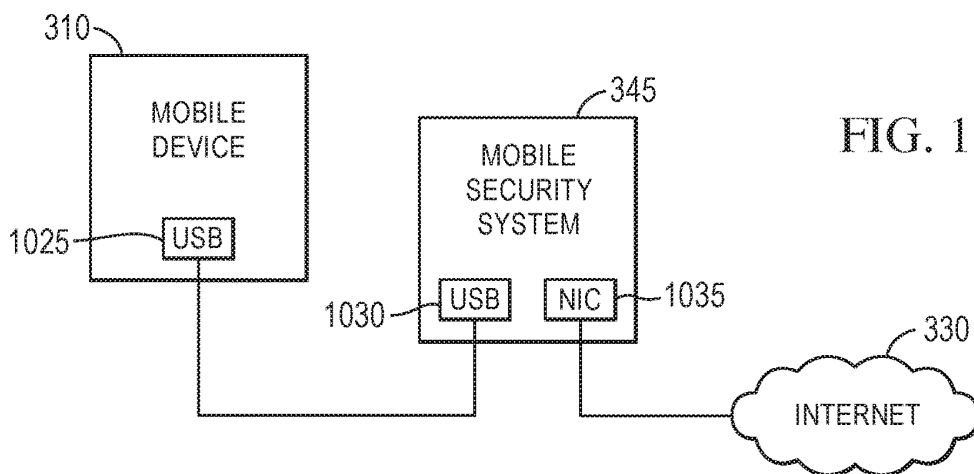
**Apr. 14, 2020**

**Sheet 10 of 10**

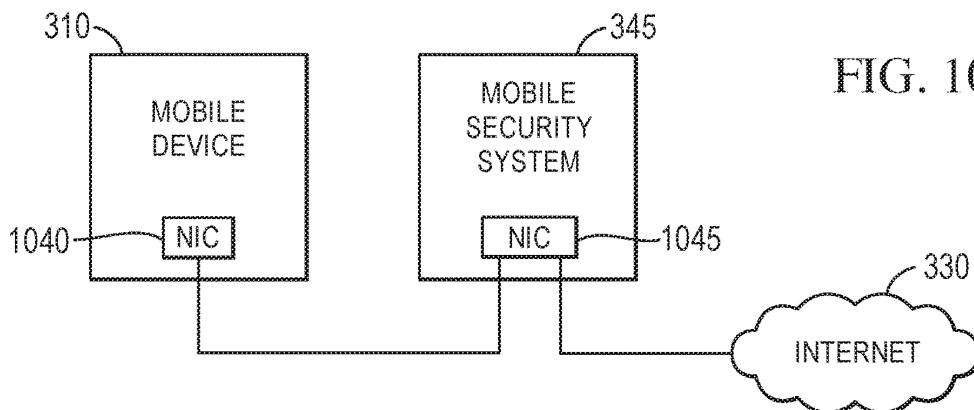
**US 10,621,344 B2**



**FIG. 10A**



**FIG. 10B**



**FIG. 10C**

US 10,621,344 B2

1

# SYSTEM AND METHOD FOR PROVIDING NETWORK SECURITY TO MOBILE DEVICES

## CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. patent application Ser. No. 16/573,877, filed Sep. 17, 2019 and entitled "System and Method for Providing Network Security to Mobile Devices," which is a continuation of U.S. patent application Ser. No. 16/144,408, filed Sep. 27, 2018 and entitled "System and Method for Providing Network Security to Mobile Devices," now U.S. Pat. No. 10,417,421, U.S. patent application Ser. No. 15/689,795, filed Aug. 29, 2017 and entitled "System and Method for Providing Network Security to Mobile Devices," now U.S. Pat. No. 10,089,462, which is a continuation of U.S. patent application Ser. No. 15/586,176, filed May 3, 2017 and entitled "System and Method for Providing Network Security to Mobile Devices," now U.S. Pat. No. 9,747,444, which is a continuation of U.S. patent application Ser. No. 15/352,553, filed Nov. 15, 2016 and entitled "System and Method for Providing Network Security to Mobile Devices," now U.S. Pat. No. 9,781,164, which is a continuation U.S. patent application Ser. No. 14/092,756, filed Nov. 27, 2013 and entitled "System and Method for Providing Network Security to Mobile Devices," now U.S. Pat. No. 9,497,622, which is a continuation of U.S. patent application Ser. No. 13/735,836, filed Jan. 7, 2013 and entitled "System and Method for Providing Network Security to Mobile Devices," now U.S. Pat. No. 8,627,452, which is a continuation of U.S. patent application Ser. No. 11/376,919, filed Mar. 15, 2006 and entitled "System and Method for Providing Network Security to Mobile Devices," now U.S. Pat. No. 8,381,297, which claims priority to U.S. Provisional Patent Application Ser. No. 60/750,326, filed Dec. 13, 2005 and entitled "Personal Security Appliance." All of the above applications are hereby incorporated by reference herein.

## TECHNICAL FIELD

This invention relates generally to network security, and more particularly provides a system and method for providing network security to mobile devices.

## BACKGROUND

The internet is an interconnection of millions of individual computer networks owned by governments, universities, nonprofit groups, companies and individuals. While the internet is a great source of valuable information and entertainment, the internet has also become a major source of system damaging and system fatal application code, such as "viruses," "spyware," "adware," "worms," "Trojan horses," and other malicious code.

To protect users, programmers design computer and computer-network security systems for blocking malicious code from attacking both individual and network computers. On the most part, network security systems have been relatively successful. A computer that connects to the internet from within an enterprise's network typically has two lines of defense. The first line of defense includes a network security system, which may be part of the network gateway, that includes firewalls, anti-virus, anti-spyware and content filtering. The second line of defense includes individual security software on individual machines, which is not typically

2

as secure as the network security system and is thus more vulnerable to attacks. In combination, the first and second lines of defense together provide pretty good security protection. However, when a device connects to the internet without the intervening network security system, the device loses its first line of defense. Thus, mobile devices (e.g., laptops, desktops, PDAs such as RIM's Blackberry, cell phones, any wireless device that connects to the internet, etc.) when traveling outside the enterprise network are more vulnerable to attacks.

FIG. 1 illustrates an example network system 100 of the prior art. Network system 100 includes a desktop 105 and a mobile device 110, each coupled to an enterprise's intranet 115. The intranet 115 is coupled via a network security system 120 (which may be a part of the enterprise's gateway) to the untrusted internet 130. Accordingly, the desktop 105 and mobile device 110 access the internet 130 via the network security system 120. A security administrator 125 typically manages the network security system 120 to assure that it includes the most current security protection and thus that the desktop 105 and mobile device 110 are protected from malicious code. Demarcation 135 divides the trusted enterprise 140 and the untrusted public internet 130. Because the desktop 105 and the mobile device 110 are connected to the internet 130 via the network security system 120, both have two lines of defense (namely, the network security system 120 and the security software resident on the device itself) against malicious code from the internet 130. Of course, although trusted, the intranet 115 can also be a source of malicious code.

FIG. 2 illustrates an example network system 200 of the prior art, when the mobile device 110 has traveled outside the trusted enterprise 140 and reconnected to the untrusted internet 130. This could occur perhaps when the user takes mobile device 110 on travel and connects to the internet 130 at a cybercafe, at a hotel, or via any untrusted wired or wireless connection. Accordingly, as shown, the mobile device 110 is no longer protected by the first line of defense (by the network security system 120) and thus has increased its risk of receiving malicious code. Further, by physically bringing the mobile device 110 back into the trusted enterprise 140 and reconnecting from within, the mobile device 110 risks transferring any malicious code received to the intranet 115.

As the number of mobile devices and the number of attacks grow, mobile security is becoming increasingly important. The problem was emphasized in the recent Info-Security Conference in New York on Dec. 7-8, 2005. However, no complete solutions were presented.

There is a need for personal security appliances capable of providing levels of network security as provided by enterprise network security systems.

## SUMMARY

An embodiment of the present invention uses a small piece of hardware that connects to a mobile device and filters out attacks and malicious code. The piece of hardware may be referred to as a "mobile security system" or "personal security appliance." Using the mobile security system, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.

In an embodiment, a mobile security system includes a connection mechanism for connecting to a data port of a mobile device and for communicating with the mobile device; a network connection module for acting as a gate-

US 10,621,344 B2

3

way to a network; a security policy for determining whether to forward content intended for the mobile device to the mobile device; and a security engine for executing the security policy.

The connection mechanism may include at least one of a USB connector, a PCMCIA connector, an Ethernet connector, and a Bluetooth communication module. The network connection module may include a network interface card that implements WiFi, WiMAX, GPRS, GSM, UMTS, CDMA, Generation 3, other cell phone internet connection protocols, etc. The security engine may include at least one of an antivirus engine, an antispyware engine, a firewall engine, an IPS/IDS engine, a content filtering engine, a multilayered security monitor, a bytecode monitor, and a URL monitor. The security policy may perform weighted risk analysis based on content type, content source, content category, or historical actions of the user. The remote management module may be capable of receiving security policy updates, security engine updates, and security data updates (including malicious content signatures). The mobile security system may include a distribution module capable of forwarding updates to other mobile security systems, and/or a backup module capable of storing at least a portion of the boot sector of the mobile device should the boot sector of the mobile device become compromised. The mobile security system may include a remote configuration module capable of communicating with a wizard, the wizard being in communication with an enterprise network security system, the wizard capable of substantially automatic generation of policies and data based on the policies and data on the enterprise network security system, the remote configuration module capable of installing the policies and data generated by the wizard. The mobile security system may include a preboot memory that is not accessible during runtime, the preboot memory storing a copy of at least a portion of the operating system of the mobile security system, the mobile security system being configured to load the operating system portion every time the mobile security system is rebooted.

In another embodiment, a method comprises receiving a network connection request from a mobile device outside of a trusted network; acting as a gateway to a network on behalf of the mobile device; receiving information intended for the mobile device from the network; and determining whether to forward the information to the mobile device in accordance with a security policy.

In another embodiment, a mobile security system comprises means for acting as a gateway to a network on behalf of a mobile device outside of a trusted network; receiving information intended for the mobile device from the network; and determining whether to forward the information to the mobile device in accordance with a security policy.

In yet another embodiment, a method comprises receiving internet traffic on a mobile device via a wireless connection; redirecting the internet traffic at the kernel level to a mobile security system; scanning the internet traffic for violations of a security policy; cleaning the internet traffic of any violations of the security policy to generate cleaned internet traffic; and sending the cleaned internet traffic to the mobile device for execution.

In still another embodiment, a system comprises a wireless network interface card on a mobile device for receiving internet traffic; a kernel-level redirector on the mobile device for redirecting the internet traffic at the kernel level to a mobile security system; a security engine for scanning the internet traffic for violations of a security policy and for cleaning the internet traffic of any violations of the security

4

policy to generate cleaned internet traffic; and a connection mechanism for receiving the redirected internet traffic from the kernel-level redirector and for sending the cleaned internet traffic to the mobile device for execution.

#### BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a prior art network system in a first state.

FIG. 2 is a block diagram of a prior art network system in a second state.

FIG. 3 is a block diagram of a network system in accordance with an embodiment of the present invention.

FIG. 4 is a block diagram illustrating details of a computer system in accordance with an embodiment of the present invention.

FIGS. 5 and 5A are block diagrams illustrating details of the mobile security system in accordance with an embodiment of the present invention.

FIG. 6 is a block diagram illustrating details of the mobile security system in accordance with a Microsoft Windows' embodiment.

FIG. 7 is a block diagram illustrating details of a smart policy updating system in accordance with an embodiment of the present invention.

FIG. 8 is a block diagram illustrating details of network security measures relative to the OSI layers.

FIG. 9 is a block diagram illustrating details of the communication technique for spreading security code to the mobile security systems.

FIGS. 10A-10C are block diagrams illustrating various architectures for connecting a mobile device to a mobile security system, in accordance with various embodiments of the present invention.

#### DETAILED DESCRIPTION

The following description is provided to enable any person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the embodiments may be possible to those skilled in the art, and the generic principles defined herein may be applied to these and other embodiments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles, features and teachings disclosed herein.

An embodiment of the present invention uses a small piece of hardware that connects to a mobile device and filters out attacks and malicious code. The piece of hardware may be referred to as a "mobile security system" or "personal security appliance." Using the mobile security system, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.

FIG. 3 illustrates a network system 300 in accordance with an embodiment of the present invention. Network system 300 includes a desktop 305, a first mobile device 310a, and a second mobile device 310b. The first mobile device 310a is illustrated as within the enterprise network 340 at this time and is coupled via a mobile security system 345a to the enterprise's intranet 315. The desktop 305 and second mobile device 310b are also within the enterprise network 340 but in this embodiment are coupled to the intranet 315 without an intervening mobile security system 345 such as mobile security system 345b. The intranet 315

US 10,621,344 B2

5

is coupled via a network security system 320 (which may be part of the enterprise's gateway) to the untrusted internet 330. Accordingly, the first mobile device 310a, the second mobile device 310b and the desktop 305 access the untrusted internet 330 via the network security system 320. Each may also be protected by a personal security system resident thereon (not shown). A third mobile device 310c is currently outside the enterprise network 340 and is coupled via a mobile security system 345b to the untrusted internet 330. The third mobile device 310 may be in use by an employee of the trusted enterprise 340 who is currently on travel. A security administrator 325 manages the mobile security system 345a, the mobile security system 345b, and the network security system 320 to assure that they include the most current security protection. One skilled in the art will recognize that the same security administrator need not manage the various devices. Further, the security administrator could be the user and need not be within the trusted enterprise 340.

Demarcation 335 divides the trusted enterprise 340 and the untrusted publicly accessible internet 330. Each of mobile device 310a, 310b and 310c may be referred to generically as mobile device 310, although they need not be identical. Each mobile security system 345a and 345b may be referred to generically as mobile security system 345, although they need not be identical.

As shown, although the mobile device 310c has traveled outside the trusted enterprise 340, the mobile device 310c connects to the untrusted internet 330 via the mobile security system 345b and thus retains two lines of defense (namely, the mobile security system 345b and the security software resident on the device itself). In this embodiment, the mobile security system 345 effectively acts as a mobile internet gateway on behalf of the mobile device 310c. In an embodiment, the mobile security system 345 may be a device dedicated to network security. In an embodiment, each mobile security system 345 may support multiple mobile devices 310, and possibly only registered mobile devices 310, e.g., those belonging to enterprise 340.

Each mobile security system 345 (e.g., 345a, 345b) may be a miniature server, based on commercial hardware (with Intel's Xscale as the core), Linux OS and network services, and open-source firewall, IDS/IPS and antivirus protection. The mobile security system 345 may be based on a hardened embedded Linux 2.6.

In this embodiment, because the security administrator 325 is capable of remotely communicating with the mobile security system 345b, IT can monitor and/or update the security policies/data/engines implemented on the mobile security system 345b. The security administrator 325 can centrally manage all enterprise devices, remotely or directly. Further, the security administrator 325 and mobile security systems 345 can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security systems 345 accordingly. Because the mobile security system 345 may be generated from the relevant security policies of the enterprise 340, the mobile device 310c currently traveling may have the same level of protection as the devices 305/310 within the trusted enterprise 340.

The mobile security system 345 may be designed as an add-on to existing software security or to replace all security hardware and software on a traveling mobile device. These security applications will preferably operate on different OSI layers to provide maximum security and malicious code detection, as shown in the example system illustrated in FIG. 8. Operating on the lower OSI layers and doing TCP/IP

6

packets analysis only (by screening firewall or router packets) would miss virus and/or worm behavior. Also, many modern viruses use mobile code implemented on a "higher" level than the 7<sup>th</sup> OSI layer (Application—HTTP, FTP, etc.) and therefore cannot be interpreted at the packet layer nor at the application layer. For example, applying antivirus analysis only at the session or transport layer on a malicious Java Script (that is included in an HTML page), trying to match the signature with packets and without understanding the content type (Java Script), will not detect the malicious nature of the Java Script. To offer greater protection, the mobile security system 345 may act as corporate class security appliance and engage different security applications based on the content type and the appropriate OSI layers, (or even a "higher" level if content is encapsulated in the application layer). The mobile security system 345 may be configured to perform content analysis at different OSI layers, e.g., from the packet level to the application level. It will be appreciated that performing deep inspection at the application level is critical to detect malicious content behavior and improve detection of viruses, worms, spyware, Trojan horses, etc. The following software packages may be implemented on the mobile security system 345:

Firewall and VPN—including stateful and stateless firewalls, NAT, packet filtering and manipulation, DOS/DDOS, netfilter, isolate user mobile devices from the internet and run VPN program on the device, etc.

Optional web accelerator and bandwidth/cache management based on Squid.

IDS/IPS—Intrusion detection and prevention system based on Snort. Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol- and anomaly-based inspections.

Antivirus and antispyware based on ClamAV; additional AV and AS engines, e.g., McAfee, Kaspersky, Pandam, may be offered for additional subscription fees.

Malicious Content Detection—on the fly heuristics that perform content analysis to detect malicious content before having signatures. This will be based on a rule base and updated rules and will be content dependent scanning.

URL Categorization Filtering—based on a commercial engine, such as Surfcontrol, Smart Filters or Websense. May provide around 70 categories of URLs such as gambling, adult content, news, webmail, etc. The mobile device 345 may apply different security policies based on the URL category, e.g., higher restriction and heuristics for Gambling or Adult content web sites, etc.

FIG. 4 is a block diagram illustrating details of an example computer system 400, of which each desktop 305, mobile device 310, network security system 320, mobile security system 345, and security administrator 325 may be an instance. Computer system 400 includes a processor 405, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a communications channel 410. The computer system 400 further includes an input device 415 such as a keyboard or mouse, an output device 420 such as a cathode ray tube display, a communications device 425, a data storage device 430 such as a magnetic disk, and memory 435 such as Random-Access Memory (RAM), each coupled to the communications channel 410. The communications interface 425 may be coupled directly or via a mobile security system 345 to a network such as the internet. One skilled in the art will recognize that, although the data storage device 430 and memory 435 are

US 10,621,344 B2

7

illustrated as different units, the data storage device **430** and memory **435** can be parts of the same unit, distributed units, virtual memory, etc.

The data storage device **430** and/or memory **435** may store an operating system **440** such as the Microsoft Windows XP, the IBM OS/2 operating system, the MAC OS, UNIX OS, LINUX OS and/or other programs **445**. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. An embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, possibly using object oriented programming methodology.

One skilled in the art will recognize that the computer system **400** may also include additional information, such as network connections, additional memory, additional processors, LANs, input/output lines for transferring information across a hardware channel, the internet or an intranet, etc. One skilled in the art will also recognize that the programs and data may be received by and stored in the system in alternative ways. For example, a computer-readable storage medium (CRSM) reader **450** such as a magnetic disk drive, hard disk drive, magneto-optical reader, CPU, etc. may be coupled to the communications bus **410** for reading a computer-readable storage medium (CRSM) **455** such as a magnetic disk, a hard disk, a magneto-optical disk, RAM, etc. Accordingly, the computer system **400** may receive programs and/or data via the CRSM reader **450**. Further, it will be appreciated that the term "memory" herein is intended to cover all data storage media whether permanent or temporary.

FIG. 5 is a block diagram illustrating details of the mobile security system **345** in accordance with an embodiment of the present invention. Mobile security system **345** includes adapters/ports/drivers **505**, memory **510**, a processor **515**, a preboot flash/ROM memory module **520** storing a secure version of the mobile security system's operating system and other applications, network connection module **525**, security engines **530**, security policies **535**, security data **540**, remote management module **550**, distribution module **555**, and backup module **560**. Although these modules are illustrated as within the mobile security system **345**, one skilled in the art will recognize that many of them could be located elsewhere, e.g., on the security administrator **325** or on third-party systems in communication with the mobile security system **345**. The mobile security system **345** may be in a pocket-size, handheld-size or key-chain size housing, or possibly smaller. Further, the mobile security system **345** may be incorporated within the mobile device **310**.

The adapters/ports/drivers **505** include connection mechanisms (including software, e.g., drivers) for USB, Ethernet, WiFi, WiMAX, GSM, CDMA, Bluetooth, PCMCIA and/or other connection data ports on the mobile security system **345**. In one embodiment, the adapters/ports/drivers **505** may be capable of connection to multiple devices **310** to provide network security to the multiple devices **310**.

Memory **510** and processor **515** execute the operating system and applications on the mobile security system **345**. In this example, the preboot flash **520** stores the operating system and applications. At boot time, the operating system and applications are loaded from the preboot flash **520** into memory **510** for execution. Since the operating system and applications are stored in the preboot flash **520**, which cannot be accessed during runtime by the user, the operating system and applications in the preboot flash **520** are not corruptible. Should the copy of the operating system and applications in memory **510** be corrupted, e.g., by malicious code, the operating system and applications may be reloaded

8

into the memory **510** from the preboot flash **520**, e.g., upon restart. Although described as stored within the preboot flash **520**, the OS and applications can be securely stored within other read-only memory devices, such as ROM, PROM, EEPROM, etc.

As shown in FIG. 5A, memory (including memory **510** and preboot flash **520**) on the mobile security system **345** may be divided into the following zones: read only memory **570**; random access memory **575** for storing a copy of the OS, kernel and security applications; runtime environment **580**; and database **585** for storing application data, log files, etc. Upon each "hard" restart, the boot loader (resident in read only memory **570**) of the mobile security system **345** copies the kernel and security applications (a fresh unchanged copy) from read only memory **570** to random access memory **575**. This causes a clean version of the OS and applications to be loaded into random access memory **575** each time. That way, if a special attack on mobile security system **345** is developed, the attack will be unable to infect the system, since the OS and applications are precluded from accessing read only memory **570** during runtime. Further, any attack that does reach memory **510** will be able to run only once and will disappear upon a hard restart. A triggering mechanism may be available to restart the mobile security system **345** automatically upon infection detection.

The network connection module **525** enables network connection, e.g., to the internet **330** or the intranet **315** via network communication hardware/software including WiFi, WiMAX, CDMA, GSM, GPRS, Ethernet, modem, etc. For example, if the mobile device **310** wishes to connect to the internet **330** via a WiFi connection, the adapters/ports/drivers **505** may be connected to the PCI port, USB port or PCMCIA port of the mobile device **310**, and the network connection module **525** of the mobile security system **345** may include a WiFi network interface card for connecting to wireless access points. Using the network connection module **425**, the mobile security system **345** may communicate with the network as a secure gateway for the mobile device **310**. Other connection architectures are described in FIGS. 10A-10C.

The security engines **530** execute security programs based on the security policies **535** and on security data **540**, both of which may be developed by IT managers. Security engines **530** may include firewalls, VPN, IPS/IDS, antivirus, anti-spyware, malicious content filtering, multilayered security monitors, Java and bytecode monitors, etc. Each security engine **530** may have dedicated security policies **535** and security data **540** to indicate which procedures, content, URLs, system calls, etc. the engines **530** may or may not allow. The security engines **530**, security policies **535** and security data **540** may be the same as, a subset of, and/or developed from the engines, policies and data on the network security system **320**.

To provide a higher security level provided by antivirus and antispyware software, the security engines **530** on each mobile security system **345** may implement content analysis and risk assessment algorithms. Operating for example at OSI Layer 7 and above (mobile code encapsulated within Layer 7), these algorithms may be executed by dedicated High Risk Content Filtering (HRCF) that can be controlled by a rules engine and rule updates. The HRCF will be based on a powerful detection library that can perform deep content analysis to verify real content types. This is because many attacks are hidden within wrong mime types and/or may use sophisticated tricks to present a text file type to a dangerous active script or ActiveX content type. The HRCF

US 10,621,344 B2

9

may integrate with a URL categorization security engine 530 for automatic rule adjustment based on the URL category. In one embodiment, when the risk level increases (using the described mechanism) the mobile security system 345 may automatically adjust and increase filtering to remove more active content from the traffic. For example, if greater risk is determined, every piece of mobile code, e.g., Java script, VB script, etc. may be stripped out.

Three aspects for integration with corporate policy server legacy systems include rules, LDAP and active directory, and logging and reporting as discussed below. In one embodiment, a policy import agent running on the security administrator 325 will access the rule base of Checkpoint Firewall-1 and Cisco PIX Firewalls and import them into a local copy. A rule analysis module will process the important rules and will offer out-of-the-box rules and policies for mobile security systems 345. This proposed policy will offer all mobile security systems 345 a best fit of rules that conform the firewall policy of the enterprise 340. The agent will run periodically to reflect any changes and generate updates for mobile security system 345 policies 535. The LDAP and Active Directory may be integrated with the directory service to maintain mobile security system 345 security policies 535 that respond to the enterprise's directory definitions. For example, a corporate policy for LDAP user Group "G" may automatically propagate to all mobile security systems 345 in "G" group. Mobile security system 345 local logs and audit trails may be sent in accordance to a logging and reporting policy to a central log stored at the security administrator 325. Using a web interface, IT may be able to generate reports and audit views related to all mobile device 310 users, their interne experiences, and attempts to bring infected devices back to the enterprise 340. IT will be able to forward events and log records into legacy management systems via SYSLOG and SNMP Traps.

The security engines 530 may perform weighted risk analysis. For example, the security engine 530 may analyze HTTP, FTP, SMTP, POP3, IM, P2P, etc. including any traffic arriving from the internet 330. The security engine 530 may assign a weight and rank for every object based on its type, complexity, richness in abilities, source of the object, etc. The security engine 530 may assign weight based on the source using a list of known dangerous or known safe sources. The security engine 530 may assign weight to objects based on the category of the source, e.g., a gambling source, an adult content source, a news source, a reputable company source, a banking source, etc. The security engine 530 may calculate the weight, and based on the result determine whether to allow or disallow access to the content, the script to run, the system modification to occur, etc. The security engine 530 may "learn" user content (by analyzing for a predetermined period of time the general content that the user accesses) and accordingly may create personal content profiles. The personal content profile may be used to calibrate the weight assigned to content during runtime analysis to improve accuracy and tailor weighted risk analysis for specific user characteristics.

In some embodiments, the security engines 530, security policies 535 and security data 540 may enable bypassing the mobile security system 345. The security policy 535, set by the security administrator 325, may include a special attribute to force network connection through the mobile security system 325 when outside the trusted enterprise 340. Thus, if this attribute is set "on," when a mobile device 310 attempts to connect to the internet 330 without the mobile security system 345 and not from within the trusted enterprise 340, all data transfer connections including LAN

10

connection, USB-net, modem, Bluetooth, WiFi, etc. may be closed. The mobile device 310 may be totally isolated and unable to connect to any network, including the internet 330.

In one embodiment, to enable this, when first connecting the mobile security system 345 to the mobile device 310 using for example the USB cable (for both power and USB connection creation), the USB plug & play device driver will be sent into the mobile device 310. The installed driver may be "Linux.inf" which allows a USB-net connection for the mobile security system 345. This connection allows the mobile security system 345 to access the internet 330 via the USB port and using the mobile device 310 network connection plus additional code ("the connection client"). In a Windows example, the connection client may be installed at the NDIS level of the mobile device 310 above all the network interface cards of every network connection as shown in FIG. 6. The implementation will be as an NDIS Intermediate (IM) Driver or NDIS-Hooking Filter Driver. Both implementations may be at the kernel level, so that an end user cannot stop or remove it. When starting the mobile device 310, the connection client may attempt to connect to the security administrator 325 or the network security system 320 locally within the trusted enterprise 340. If the node is not found (finding via VPN is considered as not found in local LAN), the connection client will assume it is working from outside the trusted enterprise 340 and expects to find the mobile security system 345 connected, e.g., via USB-net or other connection mechanism. If the mobile security system 345 is not found, the connection client may avoid any communication to any network connection. By a policy definition, this behavior can be modified to allow communication to the enterprise 340 via VPN installed in the mobile device 310. Similarly, in case of a mobile device system 345 failure, all traffic may be disabled, except for the VPN connection into the enterprise 340.

It will be appreciated that NDIS is one possible implementation of intercepting traffic at the kernel level. For example, in another embodiment, the system may hook Winsock or apply other ways that may be in future Windows versions.

In an embodiment where the mobile security system 345 supports multiple mobile devices 310, the security engines 530, security policies 535 and security data 540 may be different for each mobile device 310 (e.g., based on for example user preferences or IT decision). Alternatively, it can apply the same engines 530, policies 535 and data 540 for all connected devices 310.

The remote management module 550 enables communication with security administrator 325 (and/or other security administrators), and enables local updating of security engines 530, security policies 535, security data 540 including signatures and other applications. In one embodiment, modification to the security policies 535 and data 540 can be done by the security administrator 325 only. The remote management module 550 of the mobile security system 345 may receive updates from an update authorities device (UAD), e.g., on the security administrator 325 via a secured connection. A UAD may operate on an update server at a customer IT center located on the internet 330 to forward updates to mobile security systems 345 that possibly do not belong to an enterprise 540 in charge of managing updates. A UAD may operate on a mobile security system 345. Security engine 530 updates may modify the antivirus engine DLL, etc. OS and security application updates may be implemented only from within the enterprise 540 while connecting to the security administrator 325 and via an encrypted and authenticated connection.

TREND MICRO

EXHIBIT 1001 - PAGE 19

Appx68

## US 10,621,344 B2

11

The security administrator 325 can modify URL black and white lists for remote support to traveling users. In case of false positives, the security administrator 325 may allow access to certain URLs, by bypassing the proactive heuristics security but still monitoring by firewall, antivirus, IPS/IDS, etc. Additional remote device-management features may enable the security administrator 325 to perform remote diagnostics, access local logs, change configuration parameters, etc. on the mobile security system 345. The security administrator 325 may delegate tasks to a helpdesk for support.

The remote management module 550 may communicate with a wizard (e.g., wizard 745), which may be on the security administrator 325, as illustrated in FIG. 7, or on another system. Details of the wizard 745 and details of the communication schemes between the remote management module 550 and the wizard 745 are described below with reference to FIG. 7.

The distribution module 555 enables distribution of updates, e.g., security policy 535 updates including rule updates, security data 540 updates including signature updates, security engine 530 updates, application/OS updates, etc. by the mobile security system 345 to N other mobile security systems 345. A routing table identifying the N other mobile security systems 345 to whom to forward the updates may be provided to the distribution module 555 to enable system 345 to system 345 communication. Updates may be implemented according to policies set by the security administrator 325. When forwarding updates, the distribution module 555 acts as a UAD.

Each mobile security system 345 may obtain its routing table with security information updates, periodically, at predetermined times, upon login, etc. The routing tables may be maintained on a server, e.g., the security administrator 325 or another mobile security system 345. In one embodiment, the mobile security systems 345 may contact the server to retrieve the routing tables. Alternatively, the server may push the routing tables to the mobile security systems 345.

The distribution module 555 may enable rapid updates as shown in FIG. 9. Currently, all commercial antivirus products available do not update devices faster than viruses spread. To assure that a new virus attack does not spread faster than for example signature updates, each mobile security system 345 may be an active UAD. In one embodiment, as shown in FIG. 9, each mobile security system 345 is responsible for forwarding the signature updates to four other devices 345. As one skilled in the art will recognize, all devices 345 need to forward to the same number of other devices 345. Multiple devices 345 may be responsible for forwarding to the same device 345. When necessary, offline devices 345 being activated may poll the server, e.g., the security administrator 325, for routing table updates. Many other updating techniques are also possible.

The backup module 560 may constantly backup image and changes of the boot sector and system files of the mobile device 310 into the flash memory 520 or into another persistent memory device. That way, in case of major failure, including a loss of the system or boot sector of the mobile device 310, the mobile security system 345 may be identified as a CD-ROM during reboot and may launch the backup module (or separate program) to restore the boot sector and system files on the mobile device 310, thereby recovering the mobile device 310 without the need for IT support. In an embodiment where the network security system 345 supports multiple mobile devices 310, the

12

backup module 560 may contain separate boot sector and system files for each of the mobile devices 310, if different.

FIG. 7 is a block diagram illustrating details of a smart policy updating system 700 in accordance with an embodiment of the present invention. System 700 includes the security administrator 325 coupled to the network security system 320 and to the mobile security system 345. The network security system 320 includes security engines 705, including an antivirus engine 715, an IPS/IDS engine 720, a firewall engine 725, and other security engines. The network security system 320 also includes security policies and data 710, including antivirus policies and data 730, IPS/IDS policies and data 735, firewall policies and data 740, and other policies and data. Similarly, the mobile security system 345 includes an antivirus engine 755, an IPS/IDS engine 760, a firewall engine 765, and other engines. The mobile security system 345 also includes security policies and data 535/540, including antivirus security policies and data 770, IPS/IDS security policies and data 775, firewall security policies and data 780, and other security policies and data.

The security administrator 325 includes a wizard 745 for enabling substantially automatic initial and possibly dynamic setup of the security engines 530, security policies 535 and security data 540 on the mobile security system 345. In one embodiment, the wizard 745 may automatically load all security engines 705 and policies and data 710 of the network security system 320 as the security engines 530 and policies and data 535/540 on the mobile security system 345. In another embodiment, the wizard 745 may include all security engines 705 and policies and data 710 except those known to be irrelevant, e.g., those related to billing software used by accounting, those relating to web software running only on the web servers, etc. In another embodiment, the engines 530 would need to be loaded by an IT manager, and would not be loaded automatically by the wizard 745.

In one embodiment, the wizard 745 may determine whether the mobile security system 345 requires a particular security engine 530, e.g., an antivirus engine 755, IPS/IDS engine 760, firewall engine 765, etc. If so determined, then the wizard 745 would load the engine 530 onto the mobile security system 345. The wizard 745 would then determine which policies and data sets, e.g., some for antivirus engine 755, some for the IPS/IDS engine 760, some for the firewall engine 765, etc. are important to the mobile security system 345. The wizard 745 will then determine which of the antivirus policies and data 730 on the network security system 320 are relevant to the antivirus policies and data 770 on the mobile security system 345, which of the IPS/IDS policies and data 735 on the network security system 320 are relevant to the IPS/IDS policies and data 775 on the mobile security system 345, which of the firewall policies and data 740 on the network security system 320 are relevant to the firewall policies and data 780 on the mobile security system 345, and which of the other policies and data on the network security system 320 are relevant to the policies and data on the mobile security system 345. As stated above, the wizard 745 may determine that all security engines 705 or just a subset are needed on the mobile security system 345. The wizard 745 may determine that all policies and data 710 for a given engine type or just a subset should be forwarded. The wizard 745 may determine which relevant policies and data 710 should be forwarded to the mobile security system 345 based on rules developed by an IT manager, based on item-by-item selection during the setup procedure, etc. Alternative to the wizard 745, an IT manager can setup the engines 530 and policies and data 535/540 on the mobile security system 345 without the wizard 745.

US 10,621,344 B2

13

The security administrator 325 may also include an update authorities device 750. The update authorities device 750 may obtain security system updates (e.g., signature updates) and may send the updates to the network security system 320 and to the mobile security system 345. One skilled in the art will recognize that the updates to the network security system 320 and the updates to the mobile security system 345 need not be the same. Further, the update authorities device 750 may obtain the updates from security managers, security engine developers, antivirus specialists, etc. The update authorities device 750 may forward the updates to all network security systems 320 and all mobile security systems 345, or may forward routing tables to all mobile security systems 345 and the updates only to an initial set of mobile security systems 345. The initial set of mobile security systems 345 may forward the updates to the mobile security systems 345 identified in the routing tables in a P2P manner, similar to the process illustrated in FIG. 9. As stated above, each mobile security system 345 operating to forward updates is itself acting as an update authorities device 750.

Other applications may be included on the mobile security system 345. For example, add-on applications for recurring revenue from existing customers may include general email, anti-spam, direct and secured email delivery, information vaults, safe skype and other instant messaging services, etc.

Email Security and Anti-spam—implementation of mail relay on mobile security systems 345 (including the web security engine above) and a local spam quarantine (based on SendMail or similar process) may implement a complete mail security suite (SMTP and POP3) including anti-spam with real time indexing (via online web spam quarries). Users may have access to the quarantine to review spam messages, release messages, modify and custom spam rules, etc., via a web interface.

Direct and Secured Email Delivery based on mail relay will allow the mobile security system 345 to send user email directly from one mobile security system 345 to another mobile security system 345 without using in route mail servers. This allows corporate users to send emails that need not travel in the internet, thus leaving trace and duplicates on different unknown mail servers in route. This combined with the ability to use a secured pipe between two mobile security systems is valuable to corporations. Without such methodology, people could trace emails exchange without accessing to the enterprise's mail server, by tracking down copies in intermediate mail servers that were used to deliver the messages.

Information Vault—Application to encrypt and store end user information on the mobile security system 345 may be available only to authorized users via a web interface and a web server implemented on every mobile security system 345 (e.g., BOA, Apache, etc.).

Safe Skype and Other IM—implementing an instant messaging client on the mobile security system 345 can guarantee that the instant messaging system or P2P application has no access to data on the mobile device 310. Adding a chipset of AC/97 to provide a sound interface on the mobile security system 325 could allow users to talk and receive calls directly from/to the mobile security system 325.

Although not shown, a small battery may be included with the mobile security system 345. This battery may be charged by the USB connection during runtime or using the power adapter at any time. The battery may guarantee proper shutdown, e.g., when user disconnects the USB cable from the mobile security system 345. It will be signaled by the

14

system which will launch applications and system shutdown. This will ensure a proper state of the file system and flashing open files buffers.

A multi-layered defense and detection abilities is required. This may be done by a special code that is constantly monitoring the scanning result by different systems (antivirus, IDS/IPS, firewall, antispayware, URL category, etc.) and at different levels to build a puzzle and identify an attack even if it's not recognized by each of the individual subsystems. By doing this, the mobile security system 345 will maintain and in some cases even improve the security level provided within the enterprise 540.

One available benefit of the mobile security system 345 is its ability to enforce the policy of the enterprise 540 on the end user while they are traveling or working from home. Since the mobile security system 345 uses similar security engines and policy as when connected from within the enterprise 540 and since the end user cannot access the internet 330 without it (except via VPN connection into the enterprise 546), IT may be capable of enforcing its security policy beyond the boundaries of the enterprise 540. The OS may be under the entire supervision of IT, while the mobile security system 345 OS acts as an end user OS under his control. This resolves the problems of who controls what and how security and productivity face minimal compromise.

A standalone version of the mobile security system 345 may offer the same functionality, and may provide a local management interface via web browser. Attractive to home users and small offices that lack an IT department, the mobile security system 345 enables the end user to launch a browser, connect to the mobile security system 345, set the different policies (update policy, security rules, etc.) including modifying the white and black URL lists, etc. There is also an opportunity to provide end users with a service of remote management of the mobile security systems 345 by subscription.

FIGS. 10A, 10B and 10C illustrate three example architectures of connecting a mobile security system 345 to a mobile device 310, in accordance with various embodiments of the present invention. In FIG. 10A, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1015 and 1020 and is coupled to the internet 330 via a NIC card 1005. The mobile device 310 receives internet traffic from the internet 330 via its NIC card 1005. A kernel-level redirector 1010 (e.g., via NDIS, Winsock, etc.) on the mobile device 310 automatically redirects the internet traffic via the USB connections 1015 and 1020 to the mobile security system 345, which scans, cleans and returns the cleaned internet traffic to the mobile device 310 via the USB connections 1015 and 1020. In FIG. 10B, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1025 and 1030. The mobile security system 345 includes a NIC card 1035 for receiving internet traffic from the internet 330. The mobile security system 345 scans, cleans and forwards the internet traffic via the USB connections 1025 and 1030 to the mobile device 310. In FIG. 10C, the mobile device 310 is coupled to the mobile security system 345 via NIC cards 1040 and 1045. The mobile security system 345 receives internet traffic from the internet 330 via its NIC card 1045. The mobile security system 345 scans, cleans and forwards the internet traffic wirelessly via the NIC cards 1040 and 1045 to the mobile device 310. Other connection architectures are also possible.

The foregoing description of the preferred embodiments of the present invention is by way of example only, and other variations and modifications of the above-described embodi-

US 10,621,344 B2

15

ments and methods are possible in light of the foregoing teaching. Although the network sites are being described as separate and distinct sites, one skilled in the art will recognize that these sites may be a part of an integral site, may each include portions of multiple sites, or may include combinations of single and multiple sites. The various embodiments set forth herein may be implemented utilizing hardware, software, or any desired combination thereof. For that matter, any type of logic may be utilized which is capable of implementing the various functionality set forth herein. Components may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. Connections may be wired, wireless, modem, etc. The embodiments described herein are not intended to be exhaustive or limiting. The present invention is limited only by the following claims.

The invention claimed is:

1. A security system, comprising:

security system memory; and

a security system processor configured to:

store in the security system memory at least a portion of security code, at least a portion of a security policy, and at least a portion of security data,

the at least a portion of the security code, the at least

a portion of the security policy, and the at least a portion of the security data configured to provide

security services to a mobile device coupled to the security system, the mobile device having at least

one mobile device processor different than the security system processor of the security system,

the at least a portion of the security code, the at least a portion of the security policy, and the at least a

portion of the security data being managed by one

or more information technology (IT) administrators using an IT administrator system on a trusted

enterprise network, the at least a portion of the security code, the at least a portion of the security

policy, and the at least a portion of the security data being configured based on one or more policies

implemented by the one or more IT administrators on the trusted enterprise network, the mobile device being a first computer system, the

security system being a second computer system,

and the IT administrator system being a third computer system, the first computer system, the second computer system and the third computer

system being separate computer systems;

store in the security system memory at least a portion of remote management code configured to process an

update command, the update command being an instruction to update at least one of the security code,

the security policy, or the security data based on one or more revised policies implemented by the one or

more IT administrators on the trusted enterprise network;

receive a particular update command to update a particular one of the security code, the security policy,

or the security data, the particular update command having originated from the IT administrator system

and having been forwarded to the security system; and

execute the update command using the remote management code to update the particular one of the

security code, the security policy, or the security data.

16

2. The security system of claim 1, wherein the security system is on a separate appliance removably coupled to the mobile device.

3. The security system of claim 1, wherein the security code, the security policy, and the security data provide gateway-level security services.

4. The security system of claim 1, wherein the security code, the security policy, and the security data provide firewall security services.

5. The security system of claim 1, wherein the security code, the security policy, and the security data provide malware protection security services.

6. The security system of claim 1, wherein the security code, the security policy, and the security data provide content-based security services.

7. The security system of claim 1, wherein the IT administrator system includes an update authorities device configured to automatically generate and send update commands.

8. The security system of claim 1, wherein the security code, the security policy, and the security data are configured to mirror security policies of a gateway on the trusted enterprise network.

9. The security system of claim 1, wherein the particular update command includes a command to update configuration parameters of one of the security code, the security policy, or the security data of the security system.

10. A non-transitory computer readable storage device of a security system storing:

program instructions;

at least a portion of security code, at least a portion of a security policy, and at least a portion of security data,

the at least a portion of the security code, the at least a portion of the security policy, and the at least a

portion of the security data configured to provide security services to a mobile device coupled to the

security system, the mobile device having at least one mobile device processor different than a security

system processor of the security system,

the at least a portion of the security code, the at least a portion of the security policy, and the at least a

portion of the security data being managed by one or more information technology (IT) administrators

using an IT administrator system on a trusted enterprise network, the at least a portion of the security

code, the at least a portion of the security policy, and the at least a portion of the security data being

configured based on one or more policies implemented by the one or more IT administrators on the

trusted enterprise network, the mobile device being a first computer system, the security system being a

second computer system, and the IT administrator system being a third computer system, the first

computer system, the second computer system and the third computer system being separate computer

systems; and

at least a portion of remote management code configured to process an update command, the update command

being an instruction to update at least one of the security code, the security policy, or the security data

based on one or more revised policies implemented by the one or more IT administrators on the trusted

enterprise network;

the program instructions when executed by the security

system processor causing the security system to receive a particular update command to update a particular one of the security code, the security

## US 10,621,344 B2

17

policy, or the security data, the particular update command having originated from the IT administrator system, the particular update command having been forwarded to the security system; and

the remote management code when executed by the security system processor causing the system to process the update command to update the particular one of the security code, the security policy, or the security data.

11. The non-transitory computer readable storage device of claim 10, wherein the security system is on a separate appliance removably coupled to the mobile device.

12. The non-transitory computer readable storage device of claim 10, wherein the security code, the security policy, and the security data provide gateway-level security services.

13. The non-transitory computer readable storage device of claim 10, wherein the security code, the security policy, and the security data provide firewall security services.

14. The non-transitory computer readable storage device of claim 10, wherein the security code, the security policy, and the security data provide malware protection security services.

15. The non-transitory computer readable storage device of claim 10, wherein the security code, the security policy, and the security data provide content-based security services.

16. The non-transitory computer readable storage device of claim 10, wherein the IT administrator system includes an update authorities device configured to automatically generate and send update commands.

17. The non-transitory computer readable storage device of claim 10, wherein the security code, the security policy, and the security data are configured to mirror security policies of a gateway on the trusted enterprise network.

18. The non-transitory computer readable storage device of claim 10, wherein the particular update command includes a command to update configuration parameters of one of the security code, the security policy, or the security data of the security system.

19. A security system, comprising:

security system memory; and

a security system processor configured to:

store in the security system memory at least a portion of security code, at least a portion of a security policy, and at least a portion of security data, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to be processed by the security system processor to implement security services for a mobile device coupled to the security system, the mobile device having at least one mobile device processor different than the security system processor of the security system,

the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being managed by one or more information technology (IT) administrators using an IT administrator system on a trusted enterprise network, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network, the mobile device being a first computer system, the

18

security system being a second computer system, and the IT administrator system being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems;

store in the security system memory at least a portion of remote management code configured to process an update command, the update command being an instruction to update at least one of the security code, the security policy, or the security data based on one or more revised policies implemented by the one or more IT administrators on the trusted enterprise network;

receive a particular update command to update a particular one of the security code, the security policy, or the security data, the particular update command having originated from the IT administrator system and having been forwarded to the security system; and

execute the update command using the remote management code to update the particular one of the security code, the security policy, or the security data.

20. A non-transitory computer readable storage device of a security system storing:

program instructions;

at least a portion of security code, at least a portion of a security policy, and at least a portion of security data, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to be processed by the security system processor to implement security services for a mobile device coupled to the security system, the mobile device having at least one mobile device processor different than the security system processor of the security system,

the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being managed by one or more information technology (IT) administrators using an IT administrator system on a trusted enterprise network, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network, the mobile device being a first computer system, the security system being a second computer system, and the IT administrator system being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems; and

at least a portion of remote management code configured to process an update command, the update command being an instruction to update at least one of the security code, the security policy, or the security data based on one or more revised policies implemented by the one or more IT administrators on the trusted enterprise network;

the program instructions when executed by the security system processor causing the security system to receive a particular update command to update a particular one of the security code, the security policy, or the security data, the particular update command having originated from the IT administrator

US 10,621,344 B2

19

tor system, the particular update command having  
been forwarded to the security system; and  
the remote management code when executed by the  
security system processor causing the system to  
process the update command to update the particular 5  
one of the security code, the security policy, or the  
security data.

\* \* \* \* \*

20

**CERTIFICATE OF COMPLIANCE WITH RULE 32(B)**

1. This brief complies with the type-volume limitation of the Fed. Cir. R. 32(b) because this brief contains 9,062 words, exclusive of the items listed as exempted by Fed. R. App. P. 32(f) and Fed. Cir. R. 32(b).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally-spaced typeface using Microsoft Word in Times New Roman 14 point font.

Respectfully submitted,

Dated: March 20, 2023

By: /s/ James Hannah

Paul J. Andre  
James Hannah  
Kramer Levin Naftalis & Frankel LLP  
333 Twin Dolphin Drive, Suite 700  
Redwood Shores, CA 94065  
pandre@kramerlevin.com  
jhannah@kramerlevin.com

Jeffrey H. Price  
Kramer Levin Naftalis & Frankel LLP  
1177 Avenue of the Americas  
New York, NY 10036  
jprice@kramerlevin.com

*Attorneys for Appellant*  
CUPP Computing AS